NORME INTERNATIONALE

ISO/IEC 15408-3

Troisième édition
2008-08-15

Technologies de l'information — Techniques de sécurité — Critères d'évaluation pour la sécurité TI —

Partie 3: Composants d'assurance de sécurité

Information technology — Security techniques — Evaluation criteria for IT security —
Part 3: Security assurance components

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 15408-3:2008
https://standards.iteh.ai/catalog/standards/sist/5edd8e75-9127-414f-9a90-6dadc139a9c5/iso-iec-15408-3-2008

Numéro de référence
ISO/IEC 15408-3:2008(F)

© ISO/IEC 2008

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/IEC 15408-3:2008
https://standards.iteh.ai/catalog/standards/sist/5edd8e75-9127-414f-9a90-6dadc139a9c5/iso-iec-15408-3-2008

DOCUMENT PROTÉGÉ PAR COPYRIGHT

© ISO/IEC 2008

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
Fax: +41 22 749 09 47
E-mail: copyright@iso.org
Web: www.iso.org

Publié en Suisse

Sommaire

Page

Avant-propos ..... **ix**

Introduction ..... **xi**

1 Domaine d'application **1**

2 Références normatives **1**

3 Termes, définitions, symboles et abréviations **1**

4 Vue d'ensemble **1**
4.1 Organisation de la présente partie de l'ISO/IEC 15408 1

5 Paradigme de l'assurance **2**
5.1 Philosophie de l'ISO/IEC 15408 2
5.2 Approche de l'assurance 2
5.2.1 Importance des vulnérabilités 2
5.2.2 Origine des vulnérabilités 3
5.2.3 Assurance de l'ISO/IEC 15408 3
5.2.4 Assurance obtenue par l'évaluation 3
5.3 L'échelle ISO/IEC 15408 d'assurance de l'évaluation 4

6 Composants d'assurance de sécurité **4**
6.1 Structure des classes, des familles et des composants d'assurance de sécurité 4
6.1.1 Structure d'une classe d'assurance 4
6.1.2 Structure d'une famille d'assurance 5
6.1.3 Structure d'un composant d'assurance 6
6.1.4 Éléments d'assurance 8
6.1.5 Taxinomie d'un composant 8
6.2 Structure d'un EAL 9
6.2.1 Nom de l'EAL 9
6.2.2 Objectifs 9
6.2.3 Notes d'application 10
6.2.4 Composants d'assurance 10
6.2.5 Relation entre exigences et niveaux d'assurance 10
6.3 Structure d'un CAP 11
6.3.1 Nom d'un CAP 12
6.3.2 Objectifs 12
6.3.3 Notes d'application 12
6.3.4 Composants d'assurance 12
6.3.5 Relation entre exigences et niveaux d'assurance 13

7 Niveaux d'assurance de l'évaluation **14**
7.1 Généralités sur les niveaux d'assurance de l'évaluation (EAL) 14
7.2 Détails du niveau d'assurance de l'évaluation 15
7.3 Niveau d'assurance de l'évaluation 1 (EAL1) — testé fonctionnellement 15
7.3.1 Objectifs 15
7.3.2 Composants d'assurance 16
7.4 Niveau d'assurance de l'évaluation 2 (EAL2) — testé structurellement 16
7.4.1 Objectifs 16
7.4.2 Composants d'assurance 16
7.5 Niveau d'assurance de l'évaluation 3 (EAL3) — testé et vérifié méthodiquement 17
7.5.1 Objectifs 17
7.5.2 Composants d'assurance 18
7.6 Niveau d'assurance de l'évaluation 4 (EAL4) — conçu, testé et revu méthodiquement 19
7.6.1 Objectifs 19
7.6.2 Composants d'assurance 19
7.7 Niveau d'assurance de l'évaluation 5 (EAL5) — conçu à l'aide de méthodes semi-formelles et testé 20

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 15408-3:2008
https://standards.iteh.ai/catalog/standards/sist/5cdd8e75-9127-4141-9a90-6dadc139a9c5/iso-iec-15408-3-2008

7.7.1 Objectifs ... 20
7.7.2 Composants d'assurance ... 20
7.8 Niveau d'assurance de l'évaluation 6 (EAL6) — conception vérifiée à l'aide de méthodes semi-formelles et testé ... 21
7.8.1 Objectifs ... 21
7.8.2 Composants d'assurance ... 22
7.9 Niveau d'assurance de l'évaluation 7 (EAL7) — conception vérifiée à l'aide de méthodes formelles et testé ... 23
7.9.1 Objectifs ... 23
7.9.2 Composants d'assurance ... 23

8 Paquets d'assurance composés ... 24
8.1 Généralités sur les paquets d'assurance composés (CAP) ... 24
8.2 Détails des paquets d'assurance composés ... 26
8.3 Niveau d'assurance de la composition A (CAP-A) — composé structurellement ... 26
8.3.1 Objectifs ... 26
8.3.2 Composants d'assurance ... 26
8.4 Niveau d'assurance de la composition B (CAP-B) — composé méthodiquement ... 27
8.4.1 Objectifs ... 27
8.4.2 Composants d'assurance ... 27
8.5 Niveau d'assurance de la composition C (CAP-C) — composé, testé et revu méthodiquement ... 28
8.5.1 Objectifs ... 28
8.5.2 Composants d'assurance ... 28

9 Classe APE: Évaluation d'un profil de protection ... 29
9.1 Introduction du PP (APE_INT) ... 30
9.1.1 Objectifs ... 30
9.1.2 APE_INT.1 Introduction du PP ... 30
9.2 Revendications de conformité (APE_CCL) ... 31
9.2.1 Objectifs ... 31
9.2.2 APE_CCL.1 Revendications de conformité ... 31
9.3 Définition du problème de sécurité (APE_SPD) ... 33
9.3.1 Objectifs ... 33
9.3.2 APE_SPD.1 Définition du problème de sécurité ... 33
9.4 Objectifs de sécurité (APE_OBJ) ... 34
9.4.1 Objectifs ... 34
9.4.2 Classement des composants ... 34
9.4.3 APE_OBJ.1 Objectifs de sécurité pour l'environnement opérationnel ... 34
9.4.4 APE_OBJ.2 Objectifs de sécurité ... 34
9.5 Définition des composants étendus (APE_ECD) ... 36
9.5.1 Objectifs ... 36
9.5.2 APE_ECD.1 Définitions des composants étendus ... 36
9.6 Exigences de sécurité (APE_REQ) ... 37
9.6.1 Objectifs ... 37
9.6.2 Classement des composants ... 37
9.6.3 APE_REQ.1 Exigences de sécurité déclarées ... 37
9.6.4 APE_REQ.2 Exigences de sécurité dérivées ... 38

10 Classe ASE: Évaluation d'une cible de sécurité ... 39
10.1 Introduction de la ST (ASE_INT) ... 40
10.1.1 Objectifs ... 40
10.1.2 ASE_INT.1 Introduction de la ST ... 40
10.2 Revendications de conformité (ASE_CCL) ... 41
10.2.1 Objectifs ... 41
10.2.2 ASE_CCL.1 Revendications de conformité ... 41
10.3 Définition du problème de sécurité (ASE_SPD) ... 43
10.3.1 Objectifs ... 43
10.3.2 ASE_SPD.1 Définition du problème de sécurité ... 43
10.4 Objectifs de sécurité (ASE_OBJ) ... 44

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 15408-3:2008
https://standards.iteh.ai/catalog/standards/sist/5edd8e75-9127-414f-9a90-6dade159a9c5/iso-iec-15408-3-2008

 © ISO/IEC 2008 – Tous droits réservés

10.4.1 Objectifs ... 44
10.4.2 Classement des composants ... 44
10.4.3 ASE_OBJ.1 Objectifs de sécurité pour l'environnement opérationnel ... 44
10.4.4 ASE_OBJ.2 Objectifs de sécurité ... 44
10.5 Définitions des composants étendus (ASE_ECD) ... 46
10.5.1 Objectifs ... 46
10.5.2 ASE_ECD.1 Définition des composants étendus ... 46
10.6 Exigences de sécurité (ASE_REQ) ... 47
10.6.1 Objectifs ... 47
10.6.2 Classement des composants ... 47
10.6.3 ASE_REQ.1 Exigences de sécurité déclarées ... 47
10.6.4 ASE_REQ.2 Exigences de sécurité dérivées ... 48
10.7 Spécifications globales de la TOE (ASE_TSS) ... 49
10.7.1 Objectifs ... 49
10.7.2 Classement des composants ... 49
10.7.3 ASE_TSS.1 Spécifications globales de la TOE ... 50
10.7.4 ASE_TSS.2 Spécifications globales de la TOE avec résumé de conception architecturale ... 50

11 Classe ADV: Développement ... 51
11.1 Architecture de sécurité (ADV_ARC) ... 56
11.1.1 Objectifs ... 56
11.1.2 Classement des composants ... 56
11.1.3 Notes d'application ... 56
11.1.4 ADV_ARC.1 Description de l'architecture de sécurité ... 57
11.2 Spécifications fonctionnelles (ADV_FSP) ... 58
11.2.1 Objectifs ... 58
11.2.2 Classement des composants ... 58
11.2.3 Notes d'application ... 58
11.2.4 ADV_FSP.1 Spécification fonctionnelle de base ... 61
11.2.5 ADV_FSP.2 Spécification fonctionnelle d'application de sécurité ... 62
11.2.6 ADV_FSP.3 Spécification fonctionnelle avec résumé complet ... 63
11.2.7 ADV_FSP.4 Spécification fonctionnelle complète ... 64
11.2.8 ADV_FSP.5 Spécification fonctionnelle semi-formelle complète avec informations d'erreurs supplémentaires ... 65
11.2.9 ADV_FSP.6 Spécification fonctionnelle semi-formelle complète avec spécification formelle supplémentaire ... 66
11.3 Représentation de l'implémentation (ADV_IMP) ... 67
11.3.1 Objectifs ... 67
11.3.2 Classement des composants ... 68
11.3.3 Notes d'application ... 68
11.3.4 ADV_IMP.1 Représentation de l'implémentation de la TSF ... 69
11.3.5 ADV_IMP.2 Mappage complet de la représentation de l'implémentation de la TSF ... 70
11.4 Éléments internes de la TSF (ADV_INT) ... 71
11.4.1 Objectifs ... 71
11.4.2 Classement des composants ... 71
11.4.3 Notes d'application ... 71
11.4.4 ADV_INT.1 Sous-ensemble bien structuré d'éléments internes de la TSF ... 71
11.4.5 ADV_INT.2 Éléments internes bien structurés ... 73
11.4.6 ADV_INT.3 Éléments internes minimalement complexes ... 74
11.5 Modélisation des politiques de sécurité (ADV_SPM) ... 75
11.5.1 Objectifs ... 75
11.5.2 Classement des composants ... 75
11.5.3 Notes d'application ... 75
11.5.4 ADV_SPM.1 Modèle formel de politique de sécurité de la TOE ... 76
11.6 Conception de la TOE (ADV_TDS) ... 77
11.6.1 Objectifs ... 77
11.6.2 Classement des composants ... 77

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 15408-3:2008
https://standards.iteh.ai/catalog/standards/sist/5edd8e75-9127-414f-9a90-6dzdc139a9c5/iso-iec-15408-3-2008

11.6.3 Notes d'application ... 77
11.6.4 ADV_TDS.1 Conception de base ... 79
11.6.5 ADV_TDS.2 Conception architecturale ... 80
11.6.6 ADV_TDS.3 Conception modulaire de base ... 81
11.6.7 ADV_TDS.4 Conception modulaire semi-formelle ... 82
11.6.8 ADV_TDS.5 Conception modulaire semi-formelle complète ... 84
11.6.9 ADV_TDS.6 Conception modulaire semi-formelle complète avec présentation formelle de conception de haut niveau ... 85

12 Classe AGD: Guides ... 86
12.1 Guide opérationnel de l'utilisateur (AGD_OPE) ... 87
12.1.1 Objectifs ... 87
12.1.2 Classement des composants ... 87
12.1.3 Notes d'application ... 88
12.1.4 AGD_OPE.1 Guide opérationnel de l'utilisateur ... 88
12.2 Guide préparatoire (AGD_PRE) ... 89
12.2.1 Objectifs ... 89
12.2.2 Classement des composants ... 89
12.2.3 Notes d'application ... 90
12.2.4 AGD_PRE.1 Guide préparatoire ... 90

13 Classe ALC: Support au cycle de vie ... 91
13.1 Capacités de la CM (ALC_CMC) ... 91
13.1.1 Objectifs ... 91
13.1.2 Classement des composants ... 92
13.1.3 Notes d'application ... 92
13.1.4 ALC_CMC.1 Labellisation de la TOE ... 93
13.1.5 ALC_CMC.2 Utilisation d'un système de CM ... 93
13.1.6 ALC_CMC.3 Contrôles d'autorisation ... 94
13.1.7 ALC_CMC.4 Support à la production, procédures d'acceptation et automatisation ... 96
13.1.8 ALC_CMC.5 Support avancé ... 98
13.2 Périmètre de la CM (ALC_CMS) ... 100
13.2.1 Objectifs ... 100
13.2.2 Classement des composants ... 100
13.2.3 Notes d'application ... 101
13.2.4 ALC_CMS.1 Couverture de la CM de la TOE ... 101
13.2.5 ALC_CMS.2 Parties de la couverture de la CM de la TOE ... 101
13.2.6 ALC_CMS.3 Couverture de la CM de la représentation de l'implémentation ... 102
13.2.7 ALC_CMS.4 Couverture de la CM du suivi des problèmes ... 103
13.2.8 ALC_CMS.5 Couverture de la CM des outils de développement ... 104
13.3 Livraison (ALC_DEL) ... 105
13.3.1 Objectifs ... 105
13.3.2 Classement des composants ... 106
13.3.3 Notes d'application ... 106
13.3.4 ALC_DEL.1 Procédures de livraison ... 106
13.4 Sécurité du développement (ALC_DVS) ... 107
13.4.1 Objectifs ... 107
13.4.2 Classement des composants ... 107
13.4.3 Notes d'application ... 107
13.4.4 ALC_DVS.1 Identification des mesures de sécurité ... 107
13.4.5 ALC_DVS.2 Caractère suffisant des mesures de sécurité ... 108
13.5 Correction d'anomalies (ALC_FLR) ... 109
13.5.1 Objectifs ... 109
13.5.2 Classement des composants ... 109
13.5.3 Notes d'application ... 109
13.5.4 ALC_FLR.1 Correction d'anomalies de base ... 109
13.5.5 ALC_FLR.2 Procédures pour signaler les anomalies ... 110
13.5.6 ALC_FLR.3 Correction d'anomalies systématique ... 112

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 15408-3:2008
https://standards.iteh.ai/catalog/standards/sist/5cdd8c75-9127-414f-9a90-6daac139a9c5/iso-iec-15408-3-2008

© ISO/IEC 2008 – Tous droits réservés

13.6 Définition du cycle de vie (ALC_LCD) 114
13.6.1 Objectifs 114
13.6.2 Classement des composants 114
13.6.3 Notes d'application 114
13.6.4 ALC_LCD.1 Modèle de cycle de vie défini par le développeur 115
13.6.5 ALC_LCD.2 Modèle de cycle de vie normalisé 115
13.7 Outils et techniques (ALC_TAT) 116
13.7.1 Objectifs 116
13.7.2 Classement des composants 116
13.7.3 Notes d'application 116
13.7.4 ALC_TAT.1 Outils de développement bien définis 117
13.7.5 ALC_TAT.2 Conformité aux normes d'implémentation 118
13.7.6 ALC_TAT.3 Conformité aux normes d'implémentation - toutes les parties de la TOE 118

14 Classe ATE: Tests 119
14.1 Couverture (ATE_COV) 120
14.1.1 Objectifs 120
14.1.2 Classement des composants 120
14.1.3 Notes d'application 120
14.1.4 ATE_COV.1 Éléments de preuve de la couverture 120
14.1.5 ATE_COV.2 Analyse de la couverture 121
14.1.6 ATE_COV.3 Analyse rigoureuse de la couverture 122
14.2 Profondeur (ATE_DPT) 123
14.2.1 Objectifs 123
14.2.2 Classement des composants 123
14.2.3 Notes d'application 123
14.2.4 ATE_DPT.1 Tests: conception de base 123
14.2.5 ATE_DPT.2 Tests: modules d'application de la sécurité 124
14.2.6 ATE_DPT.3 Tests: conception modulaire 125
14.2.7 ATE_DPT.4 Tests: représentation de l'implémentation 126
14.3 Tests fonctionnels (ATE_FUN) 127
14.3.1 Objectifs 127
14.3.2 Classement des composants 127
14.3.3 Notes d'application 127
14.3.4 ATE_FUN.1 Tests fonctionnels 127
14.3.5 ATE_FUN.2 Tests fonctionnels ordonnés 128
14.4 Tests indépendants (ATE_IND) 129
14.4.1 Objectifs 129
14.4.2 Classement des composants 129
14.4.3 Notes d'application 130
14.4.4 ATE_IND.1 Tests indépendants - conformité 130
14.4.5 ATE_IND.2 Tests indépendants - échantillonnage 131
14.4.6 ATE_IND.3 Tests indépendants - totalité 132

15 Classe AVA: Estimation des vulnérabilités 133
15.1 Notes d'application 134
15.2 Analyse de vulnérabilités (AVA_VAN) 134
15.2.1 Objectifs 134
15.2.2 Classement des composants 135
15.2.3 AVA_VAN.1 Étude des vulnérabilités 135
15.2.4 AVA_VAN.2 Analyse de vulnérabilités 136
15.2.5 AVA_VAN.3 Analyse de vulnérabilités ciblée 137
15.2.6 AVA_VAN.4 Analyse de vulnérabilités méthodique 138
15.2.7 AVA_VAN.5 Analyse de vulnérabilités méthodique avancée 139

16 Classe ACO: Composition 140
16.1 Justification de la composition (ACO_COR) 143
16.1.1 Objectifs 143
16.1.2 Classement des composants 143

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 15408-3:2008
https://standards.iteh.ai/catalog/standards/sist/5ad0e75-9427-4148-9a90-6d4de139b2b5/iso-iec-15408-3-2008

16.1.3 ACO_COR.1 Justification de la composition ... 143
16.2 Preuve de développement (ACO_DEV) ... 143
16.2.1 Objectifs ... 143
16.2.2 Classement des composants ... 143
16.2.3 Notes d'application ... 144
16.2.4 ACO_DEV.1 Description fonctionnelle ... 144
16.2.5 ACO_DEV.2 Preuve de conception de base ... 145
16.2.6 ACO_DEV.3 Preuve de conception détaillée ... 146
16.3 Confiance dans les composants dépendants (ACO_REL) ... 147
16.3.1 Objectifs ... 147
16.3.2 Classement des composants ... 147
16.3.3 Notes d'application ... 147
16.3.4 ACO_REL.1 Informations de confiance de base ... 148
16.3.5 ACO_REL.2 Informations de confiance ... 148
16.4 Test de TOE composée (ACO_CTT) ... 149
16.4.1 Objectifs ... 149
16.4.2 Classement des composants ... 149
16.4.3 Notes d'application ... 149
16.4.4 ACO_CTT.1 Test d'interface ... 150
16.4.5 ACO_CTT.2 Test d'interface rigoureux ... 151
16.5 Analyse de vulnérabilité de composition (ACO_VUL) ... 152
16.5.1 Objectifs ... 152
16.5.2 Classement des composants ... 152
16.5.3 Notes d'application ... 152
16.5.4 ACO_VUL.1 Revue de vulnérabilité de composition ... 153
16.5.5 ACO_VUL.2 Analyse de vulnérabilité de composition ... 154
16.5.6 ACO_VUL.3 Analyse de vulnérabilité de composition de base améliorée ... 154

Annexe A (informative) **Développement (ADV)** ... **156**

Annexe B (informative) **Composition (ACO)** ... **175**

Annexe C (informative) **Référence croisée des dépendances entre les composants d'assurance** ... **183**

Annexe D (informative) **Référence croisée des PP et des composants d'assurance** ... **187**

Annexe E (informative) **Référence croisée des EAL et des composants d'assurance** ... **188**

Annexe F (informative) **Référence croisée des CAP et des composants d'assurance** ... **189**

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 15408-3:2008
https://standards.iteh.ai/catalog/standards/sist/5cdd8c75-9127-4141-9a90-64e3-189a9e5/iso-iec-15408-3-2008

© ISO/IEC 2008 – Tous droits réservés

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. Dans le domaine des technologies de l'information, l'ISO et l'IEC ont créé un comité technique mixte, l'ISO/IEC JTC 1.

Les Normes internationales sont rédigées conformément aux règles données dans les Directives ISO/IEC, Partie 2.

La tâche principale du comité technique mixte est d'élaborer les Normes internationales. Les projets de Normes internationales adoptés par le comité technique mixte sont soumis aux organismes nationaux pour vote. Leur publication comme Normes internationales requiert l'approbation de 75 % au moins des organismes nationaux votants.

L'attention est attirée sur le fait que certains des éléments du présent document peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. L'ISO et l'IEC ne sauraient être tenues pour responsables de ne pas avoir identifié de tels droits de propriété et averti de leur existence.

Le présent document a été élaboré par le comité technique ISO/IEC JTC 1, *Technologies de l'information*, sous-comité SC 27, *Techniques de sécurité des technologies de l'information*. Le texte identique de l'ISO/IEC 15408 est publié par les organisations commanditaires du projet Critères communs sous le titre Common Criteria for Information Technology Security Evaluation (Critères Communs pour l'évaluation de la sécurité des technologies de l'information). La source XML commune aux deux publications peut être obtenue à l'adresse http://www.oc.ccn.cni.es/xml.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 15408-3:2008
https://standards.iteh.ai/catalog/standards/sist/5cd8e75-9137-4146-9e90-6dadc139a9c5/iso-iec-15408-3-2008

Cette troisième édition annule et remplace la deuxième édition (ISO/IEC 15408-3:2005), qui a fait l'objet d'une révision technique.

L'ISO/IEC 15408 comprend les parties suivantes, présentées sous le titre général *Technologies de l'information — Techniques de sécurité — Critères d'évaluation pour la sécurité TI*:

— Partie 1: Introduction et modèle général

— Partie 2: Composants fonctionnels de sécurité

— Partie 3: Composants d'assurance de sécurité

La présente version corrigée de l'ISO/IEC 15408-3:2008 incorpore diverses corrections éditoriales principalement liées aux composants d'assurance EAL4 et EAL6, ADV_FSP, ADV_TDS, ATE_DPT.2, ATE_IND et ALC.

© ISO/IEC 2008 – Tous droits réservés

Mention légale

Les organismes gouvernementaux cités ci-dessous ont contribué au développement de la présente version des Critères Communs pour l'évaluation de la sécurité des technologies de l'information. En tant que co-titulaires du copyright relatif aux critères communs pour l'évaluation de la sécurité des technologies de l'information, version 3.1, Parties 1 à 3 (appelés CC 3.1), ils accordent par la présente une licence non exclusive à l'ISO/IEC pour utiliser les CC 3.1 dans la poursuite de l'élaboration et de la tenue à jour de la Norme internationale ISO/IEC 15408. Ces organismes gouvernementaux conservent toutefois le droit d'utiliser, de copier, de distribuer, de traduire ou de modifier les CC 3.1 comme ils l'entendent.

Australie/Nouvelle-Zélande:	Defence Signals Directorate et Government Communications Security Bureau, respectivement;
Canada:	Communications Security Establishment/Centre de la sécurité descommunications;
France:	Direction Centrale de la Sécurité des Systèmes d'Information;
Allemagne:	Bundesamt für Sicherheit in der Informationstechnik;
Japon:	Information Technology Promotion Agency;
Pays-Bas:	Netherlands National Communications Security Agency;
Espagne:	Ministerio de Administraciones Públicas et Centro Criptológico Nacional;
Royaume-Uni:	Communications-Electronic Security Group;
États-Unis:	National Security Agency et National Institute of Standards and Technology.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 15408-3:2008
https://standards.iteh.ai/catalog/standards/sist/5edd8e75-9127-414f-9a90-6dadc139a9c5/iso-iec-15408-3-2008

 © ISO/IEC 2008 – Tous droits réservés

Introduction

Les composants d'assurance de sécurité, tels que définis dans la présente partie de l'ISO/IEC 15408, servent de base aux exigences d'assurance de sécurité exprimées dans un Profil de Protection (Protection Profile ou PP) ou dans une Cible de Sécurité (Security Target ou ST).

Ces exigences établissent une façon normalisée d'exprimer les exigences d'assurance des TOE. La présente partie de l'ISO/IEC 15408 propose un catalogue de l'ensemble des composants, des familles et des classes d'assurance. La présente partie de l'ISO/IEC 15408 définit également des critères d'évaluation pour les PP et les ST, et présente les niveaux d'assurance de l'évaluation qui définissent l'échelle prédéfinie de l'ISO/IEC 15408 pour coter l'assurance pour les Cibles d'Évaluation (Targets of Évaluation ou TOE), constituée par les niveaux d'assurance de l'évaluation ou EAL (Évaluation Assurance Levels).

L'audience de la présente partie de l'ISO/IEC 15408 comprend les utilisateurs, les développeurs et les évaluateurs de produits TI sûrs. L'ISO/IEC 15408-1:2009, Article 5, donne des informations supplémentaires sur l'audience visée de l'ISO/IEC 15408 et sur l'utilisation de l'ISO/IEC 15408 par les groupes qui constituent l'audience visée. Ces groupes peuvent utiliser la présente partie de l'ISO/IEC 15408 de la façon suivante:

a) les utilisateurs qui utilisent la présente partie de l'ISO/IEC 15408 lorsqu'ils sélectionnent des composants pour exprimer des exigences d'assurance visant à satisfaire aux objectifs de sécurité exprimés dans un PP ou une ST, en déterminant les niveaux requis d'assurance de sécurité de la TOE;

iTeh STANDARD PREVIEW
(standards.iteh.ai)

b) les développeurs qui, en construisant une TOE, répondent aux exigences de sécurité réelles ou perçues des utilisateurs, se réfèrent à la présente partie de l'ISO/IEC 15408 pour interpréter les exigences d'assurance et déterminer les approches d'assurance des TOE;

ISO/IEC 15408-3:2008
https://standards.iteh.ai/catalog/standards/sist/5edd8e75-9132-414f-9a90-6dadc139a9c5/iso-iec-15408-3-2008

c) les évaluateurs, qui utilisent les exigences d'assurance définies dans la présente partie de l'ISO/IEC 15408 comme critères d'évaluation obligatoires pour déterminer le niveau d'assurance des TOE et pour évaluer les PP et les ST.

© ISO/IEC 2008 – Tous droits réservés

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/IEC 15408-3:2008
https://standards.iteh.ai/catalog/standards/sist/5edd8e75-9127-414f-9a90-6dadc139a9c5/iso-iec-15408-3-2008

Technologies de l'information — Techniques de sécurité — Critères d'évaluation pour la sécurité TI —

Partie 3: Composants d'assurance de sécurité

1 Domaine d'application

La présente partie de l'ISO/IEC 15408 définit les exigences d'assurance de l'ISO/IEC 15408. Elle comprend les niveaux d'assurance de l'évaluation (Évaluation Assurance Level, EAL) qui définissent une échelle pour mesurer l'assurance pour les cibles d'évaluation (Targets of Évaluation, TOE) des composants, les paquets d'assurance composés (Composed Assurance Packages, CAP) qui définissent une échelle pour mesurer l'assurance des TOE composées, les composants individuels d'assurance à partir desquels sont composés les niveaux et les paquets d'assurance, et les critères pour l'évaluation des profils de protection (Protection Profiles, PP) et des cibles de sécurité (Security Targets, ST).

2 Références normatives

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Les documents de référence suivants sont indispensables pour l'application 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 15408-3:2008
https://standards.iteh.ai/catalog/standards/sist/5edd8e75-9127-414f-9a90-6dadc139a9c5/iso-iec-15408-3-2008

ISO/IEC 15408-1, *Technologies de l'information — Techniques de sécurité — Critères d'évaluation pour la sécurité TI — Partie 1: Introduction et modèle général*

ISO/IEC 15408-2, *Technologies de l'information — Techniques de sécurité — Critères d'évaluation pour la sécurité TI — Partie 2: Composants fonctionnels de sécurité*

3 Termes, définitions, symboles et abréviations

Pour les besoins du présent document, les termes, définitions, symboles et abréviations de l'ISO/IEC 15408-1 s'appliquent.

4 Vue d'ensemble

4.1 Organisation de la présente partie de l'ISO/IEC 15408

L'Article 5 décrit le paradigme utilisé dans les exigences d'assurance de sécurité de la présente partie de l'ISO/IEC 15408.

L'Article 6 décrit la structure adoptée pour la présentation des classes, familles, composants d'assurance et niveaux d'assurance de l'évaluation ainsi que leurs relations, et la structure des paquets d'assurance composés. Il caractérise également les classes et familles d'assurance qui se trouvent dans les Articles 9 à 16.

L'Article 7 donne les définitions détaillées des EAL.

L'Article 8 donne les définitions détaillées des CAP.

Les Articles 9 à 16 donnent les définitions détaillées des classes d'assurance de la présente partie de l'ISO/IEC 15408.

© ISO/IEC 2008 – Tous droits réservés

L'Annexe A donne des explications supplémentaires et des exemples des concepts associés à la classe «Développement».

L'Annexe B fournit une explication des concepts associés aux évaluations de TOE composées et à la classe «Composition».

L'Annexe C contient un résumé des dépendances entre les composants d'assurance.

L'Annexe D contient les références croisées entre les PP et les familles et composants de la classe APE.

L'Annexe E contient les références croisées entre les EAL et les composants d'assurance.

L'Annexe F contient les références croisées entre les CAP et les composants d'assurance.

5 Paradigme de l'assurance

Le but du présent article est de documenter la philosophie qui étaye la manière adoptée par l'ISO/IEC 15408 pour aborder l'assurance. La compréhension du présent article permettra au lecteur d'appréhender l'argumentaire relatif aux exigences d'assurance de la présente partie de l'ISO/IEC 15408.

5.1 Philosophie de l'ISO/IEC 15408

Selon la philosophie de l'ISO/IEC 15408, il convient d'exprimer clairement les menaces qui pèsent sur la sécurité et les règles en termes de politique de sécurité organisationnelle et il convient de démontrer que les mesures de sécurité proposées sont suffisantes pour atteindre le but prévu.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

De plus, il convient d'adopter des mesures pour réduire la probabilité d'occurrence de vulnérabilités, ainsi que la capacité d'activer (c'est-à-dire d'exploiter intentionnellement ou bien de déclencher) de manière non intentionnelle une vulnérabilité, et enfin pour réduire l'étendue des dommages qui pourraient en résulter. En complément, il convient d'adopter des mesures qui facilitent l'identification ultérieure des vulnérabilités ainsi que leur élimination ou leur atténuation, et/ou la notification qu'une vulnérabilité a été exploitée ou déclenchée.

ISO/IEC 15408-3:2008
https://standards.iteh.ai/catalog/standards/iso/e7c4f7f5-2f25-4e7b-9f1b-64bdc139a9c5/iso-iec-15408-3-2008

5.2 Approche de l'assurance

Le principe de base de l'ISO/IEC 15408 consiste à fournir une assurance basée sur une évaluation (une investigation active) du produit TI auquel on doit accorder sa confiance. L'évaluation a été le moyen traditionnel de fournir l'assurance et constitue la base sur laquelle reposent les critères d'évaluation qui ont précédé l'ISO/IEC 15408. L'ISO/IEC 15408 adopte le même principe de base en mettant en commun les approches existantes. L'ISO/IEC 15408 propose de faire mesurer, par des experts en évaluation, la validité de la documentation et du produit TI qui en résulte, avec un accent croissant sur le champ d'application, la profondeur et la rigueur.

L'ISO/IEC 15408 n'exclut ni ne commente la valeur relative d'autres moyens d'obtenir l'assurance. Les recherches se poursuivent en ce qui concerne les solutions alternatives pour acquérir l'assurance. Lorsque des démarches alternatives arriveront à maturité grâce à ces recherches, l'opportunité de leur inclusion dans l'ISO/IEC 15408 sera considérée, cette norme étant structurée de façon à permettre leur introduction future.

5.2.1 Importance des vulnérabilités

On suppose qu'il existe des agents menaçants qui chercheront activement à exploiter les occasions de violer les politiques de sécurité, aussi bien pour s'assurer des gains illicites que pour commettre des actions bien intentionnées, néanmoins non sûres. Les agents menaçants peuvent aussi déclencher accidentellement des vulnérabilités de sécurité, causant ainsi des dommages à l'organisation concernée. Le besoin de traiter les informations sensibles et le manque de disponibilité de produits auxquels on peut faire suffisamment confiance, entraînent l'existence de risques significatifs, dus aux défaillances dans les TI. Il est par conséquent vraisemblable que des violations de la sécurité des TI puissent conduire à des pertes importantes.

 © ISO/IEC 2008 – Tous droits réservés

Des violations de la sécurité des TI surviennent pendant l'utilisation des TI pour des besoins professionnels, par l'exploitation intentionnelle ou le déclenchement accidentel de vulnérabilités.

Il convient de prendre des mesures pour empêcher l'apparition de vulnérabilités dans les produits TI. Dans la mesure du possible, il convient que les vulnérabilités soient:

a) éliminées — ce qui signifie qu'il convient de prendre des mesures actives pour démasquer, puis supprimer ou neutraliser, toutes les vulnérabilités susceptibles d'être mises en œuvre;

b) minimisées — ce qui signifie qu'il convient de prendre des mesures actives pour réduire l'impact potentiel de l'exploitation d'une vulnérabilité quelconque à un niveau résiduel acceptable;

c) contrôlées — ce qui signifie qu'il convient de prendre des mesures pour s'assurer que toute tentative pour exploiter une vulnérabilité résiduelle sera détectée de façon à pouvoir prendre des mesures pour limiter les dégâts.

5.2.2 Origine des vulnérabilités

Les vulnérabilités peuvent se présenter par l'intermédiaire de défaillances dans:

a) les exigences — ce qui signifie qu'un produit TI peut inclure toutes les fonctions et caractéristiques exigées et, malgré cela, contenir des vulnérabilités qui le rendent inadapté ou inefficace pour la sécurité;

b) le développement —ce qui signifie qu'un produit TI ne satisfait pas à ses spécifications et/ou que des vulnérabilités ont été introduites à cause de l'utilisation de méthodes de développement médiocres ou de choix de conception incorrects;

iTeh STANDARD PREVIEW
(standards.iteh.ai)

c) l'exploitation —ce qui signifie qu'un produit TI a été développé correctement sur la base de spécifications correctes, mais que des vulnérabilités ont été introduites à cause de contrôles non appropriés en exploitation.

ISO/IEC 15408-3:2008
https://standards.iteh.ai/catalog/standards/sist/5edd8e75-9127-414f-9a90-6dade139a9c5/iso-iec-15408-3-2008

5.2.3 Assurance de l'ISO/IEC 15408

L'assurance est le fondement de la confiance dans le fait qu'un produit TI satisfait à ses objectifs de sécurité. L'assurance peut être déduite à partir de sources telles que des affirmations non prouvées, une expérience préalable appropriée ou bien une expérience spécifique. Néanmoins, l'ISO/IEC 15408 procure l'assurance par l'intermédiaire d'investigations actives. Les investigations actives consistent en une évaluation du produit TI pour déterminer ses propriétés de sécurité.

5.2.4 Assurance obtenue par l'évaluation

L'évaluation est le moyen traditionnel pour procurer l'assurance et constitue la base de l'approche ISO/IEC 15408. Les techniques d'évaluation peuvent comprendre les éléments suivants, sans que cette liste soit exhaustive:

a) l'analyse et la vérification du ou des processus et procédures;

b) la vérification que le ou les processus et procédures sont appliqués;

c) l'analyse des correspondances entre les représentations de conception de la TOE;

d) l'analyse de chaque représentation de conception de la TOE par rapport aux exigences;

e) la vérification de preuves;

f) l'analyse de guides;

g) l'analyse de tests fonctionnels développés et des résultats obtenus;

h) les tests fonctionnels indépendants;

© ISO/IEC 2008 – Tous droits réservés