

---

---

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

**Partie 2:  
Composants fonctionnels de sécurité**

*Information technology — Security techniques — Evaluation criteria  
for IT security —*

*Part 2: Security functional components*





**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](mailto:copyright@iso.org)  
Web: [www.iso.org](http://www.iso.org)

Publié en Suisse

## Sommaire

Page

Avant-propos .....	xv
Introduction .....	xvii
<b>1</b> <b>Domaine d'application</b> .....	<b>1</b>
<b>2</b> <b>Références normatives</b> .....	<b>1</b>
<b>3</b> <b>Termes, définitions, symboles et abréviations</b> .....	<b>1</b>
<b>4</b> <b>Vue d'ensemble</b> .....	<b>1</b>
4.1    Organisation de la présente partie de l'ISO/IEC 15408 .....	1
<b>5</b> <b>Modèle d'exigences fonctionnelles</b> .....	<b>2</b>
<b>6</b> <b>Composants fonctionnels de sécurité</b> .....	<b>6</b>
6.1    Vue d'ensemble .....	6
6.1.1    Structure des classes .....	6
6.1.2    Structure d'une famille .....	6
6.1.3    Structure d'un composant .....	8
6.2    Catalogue de composants .....	10
6.2.1    Mise en évidence des changements de composants .....	11
<b>7</b> <b>Classe FAU: Audit de sécurité</b> .....	<b>11</b>
7.1    Réponse automatique de l'audit de sécurité (FAU_ARP) .....	11
7.1.1    Comportement de la famille .....	11
7.1.2    Classement des composants .....	12
7.1.3    Gestion de FAU_ARP.1 .....	12
7.1.4    Audit de FAU_ARP.1 .....	12
7.1.5    FAU_ARP.1 Alarmes de sécurité .....	12
7.2    Génération de données de l'audit de sécurité (FAU_GEN) .....	12
7.2.1    Comportement de la famille .....	12
7.2.2    Classement des composants .....	12
7.2.3    Gestion de FAU_GEN.1, FAU_GEN.2 .....	12
7.2.4    Audit de FAU_GEN.1, FAU_GEN.2 .....	12
7.2.5    FAU_GEN.1 Génération de données d'audit .....	12
7.2.6    FAU_GEN.2 Lien avec l'identité de l'utilisateur .....	13
7.3    Analyse de l'audit de sécurité (FAU_SAA) .....	13
7.3.1    Comportement de la famille .....	13
7.3.2    Classement des composants .....	13
7.3.3    Gestion de FAU_SAA.1 .....	14
7.3.4    Gestion de FAU_SAA.2 .....	14
7.3.5    Gestion de FAU_SAA.3 .....	14
7.3.6    Gestion de FAU_SAA.4 .....	14
7.3.7    Audit de FAU_SAA.1, FAU_SAA.2, FAU_SAA.3, FAU_SAA.4 .....	14
7.3.8    FAU_SAA.1 Analyse de violation potentielle .....	14
7.3.9    FAU_SAA.2 Détection d'anomalie basée sur un profil .....	15
7.3.10    FAU_SAA.3 Heuristique des attaques simples .....	15
7.3.11    FAU_SAA.4 Heuristique des attaques complexes .....	16
7.4    Revue de l'audit de sécurité (FAU_SAR) .....	16
7.4.1    Comportement de la famille .....	16
7.4.2    Classement des composants .....	16
7.4.3    Gestion de FAU_SAR.1 .....	16
7.4.4    Gestion de FAU_SAR.2, FAU_SAR.3 .....	17
7.4.5    Audit de FAU_SAR.1 .....	17
7.4.6    Audit de FAU_SAR.2 .....	17
7.4.7    Audit de FAU_SAR.3 .....	17
7.4.8    FAU_SAR.1 Revue d'audit .....	17
7.4.9    FAU_SAR.2 Revue d'audit restreinte .....	17
7.4.10    FAU_SAR.3 Revue d'audit sélective .....	17