

Third edition
2008-08-15

Corrected version
2011-06-01

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

**Part 2:
Security functional components**

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

Partie 2: Composants fonctionnels de sécurité



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2008

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword	xviii
Introduction.....	xx
1 Scope	1
2 Normative references	1
3 Terms and definitions, symbols and abbreviated terms.....	1
4 Overview.....	1
4.1 Organisation of this part of ISO/IEC 15408	1
5 Functional requirements paradigm	2
6 Security functional components.....	5
6.1 Overview.....	5
6.1.1 Class structure	5
6.1.2 Family structure.....	6
6.1.3 Component structure	8
6.2 Component catalogue.....	9
6.2.1 Component changes highlighting	10
7 Class FAU: Security audit.....	10
7.1 Security audit automatic response (FAU_ARP)	11
7.1.1 Family Behaviour.....	11
7.1.2 Component levelling	11
7.1.3 Management of FAU_ARP.1	11
7.1.4 Audit of FAU_ARP.1	11
7.1.5 FAU_ARP.1 Security alarms.....	11
7.2 Security audit data generation (FAU_GEN)	11
7.2.1 Family Behaviour.....	11
7.2.2 Component levelling	11
7.2.3 Management of FAU_GEN.1, FAU_GEN.2.....	11
7.2.4 Audit of FAU_GEN.1, FAU_GEN.2	11
7.2.5 FAU_GEN.1 Audit data generation	12
7.2.6 FAU_GEN.2 User identity association.....	12
7.3 Security audit analysis (FAU_SAA)	12
7.3.1 Family Behaviour.....	12
7.3.2 Component levelling	12
7.3.3 Management of FAU_SAA.1	13
7.3.4 Management of FAU_SAA.2	13
7.3.5 Management of FAU_SAA.3	13
7.3.6 Management of FAU_SAA.4	13
7.3.7 Audit of FAU_SAA.1, FAU_SAA.2, FAU_SAA.3, FAU_SAA.4.....	13
7.3.8 FAU_SAA.1 Potential violation analysis	13
7.3.9 FAU_SAA.2 Profile based anomaly detection	14
7.3.10 FAU_SAA.3 Simple attack heuristics	14
7.3.11 FAU_SAA.4 Complex attack heuristics.....	15
7.4 Security audit review (FAU_SAR)	15
7.4.1 Family Behaviour.....	15
7.4.2 Component levelling	15
7.4.3 Management of FAU_SAR.1	15
7.4.4 Management of FAU_SAR.2, FAU_SAR.3	15
7.4.5 Audit of FAU_SAR.1	15
7.4.6 Audit of FAU_SAR.2	16
7.4.7 Audit of FAU_SAR.3	16