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

**Part 2:
Security functional requirements**

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

Partie 2: Exigences fonctionnelles de sécurité

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

© ISO/IEC 2005

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, 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.....	6
6.1 Overview.....	6
6.1.1 Class structure	7
6.1.2 Family structure.....	7
6.1.3 Component structure	9
6.2 Component catalogue.....	10
6.2.1 Component changes highlighting	11
7 Class FAU: Security audit.....	11
7.1 Security audit automatic response (FAU_ARP)	12
7.1.1 Family Behaviour.....	12
7.1.2 Component levelling	12
7.1.3 Management of FAU_ARP.1	12
7.1.4 Audit of FAU_ARP.1.....	12
7.1.5 FAU_ARP.1 Security alarms.....	13
7.2 Security audit data generation (FAU_GEN)	13
7.2.1 Family Behaviour.....	13
7.2.2 Component levelling	13
7.2.3 Management of FAU_GEN.1, FAU_GEN.2.....	13
7.2.4 Audit of FAU_GEN.1, FAU_GEN.2	13
7.2.5 FAU_GEN.1 Audit data generation	13
7.2.6 FAU_GEN.2 User identity association.....	14
7.3 Security audit analysis (FAU_SAA)	14
7.3.1 Family Behaviour.....	14
7.3.2 Component levelling	14
7.3.3 Management of FAU_SAA.1	15
7.3.4 Management of FAU_SAA.2	15
7.3.5 Management of FAU_SAA.3	15
7.3.6 Management of FAU_SAA.4	15
7.3.7 Audit of FAU_SAA.1, FAU_SAA.2, FAU_SAA.3, FAU_SAA.4.....	15
7.3.8 FAU_SAA.1 Potential violation analysis	15
7.3.9 FAU_SAA.2 Profile based anomaly detection	16
7.3.10 FAU_SAA.3 Simple attack heuristics	16
7.3.11 FAU_SAA.4 Complex attack heuristics.....	16
7.4 Security audit review (FAU_SAR)	17
7.4.1 Family Behaviour.....	17
7.4.2 Component levelling	17
7.4.3 Management of FAU_SAR.1	17
7.4.4 Management of FAU_SAR.2, FAU_SAR.3.....	17
7.4.5 Audit of FAU_SAR.1	17
7.4.6 Audit of FAU_SAR.2	18