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

**Part 2:
Security functional requirements**

iTeh STANDARD PREVIEW
*Technologies de l'information — Techniques de sécurité — Critères
d'évaluation pour la sécurité TI —*
(standards.iteh.ai)
Partie 2: Exigences fonctionnelles de sécurité

ISO/IEC 15408-2:2005

<https://standards.iteh.ai/catalog/standards/sist/54792c7c-7a68-481c-ac16-571749da786e/iso-iec-15408-2-2005>

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[ISO/IEC 15408-2:2005](https://standards.iteh.ai/catalog/standards/sist/54792c7c-7a68-481c-ac16-571749da786e/iso-iec-15408-2-2005)

<https://standards.iteh.ai/catalog/standards/sist/54792c7c-7a68-481c-ac16-571749da786e/iso-iec-15408-2-2005>

© 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

7.4.7	Audit of FAU_SAR.3	18
7.4.8	FAU_SAR.1 Audit review	18
7.4.9	FAU_SAR.2 Restricted audit review	18
7.4.10	FAU_SAR.3 Selectable audit review	18
7.5	Security audit event selection (FAU_SEL)	19
7.5.1	Family Behaviour	19
7.5.2	Component levelling	19
7.5.3	Management of FAU_SEL.1	19
7.5.4	Audit of FAU_SEL.1	19
7.5.5	FAU_SEL.1 Selective audit	19
7.6	Security audit event storage (FAU_STG)	19
7.6.1	Family Behaviour	19
7.6.2	Component levelling	20
7.6.3	Management of FAU_STG.1	20
7.6.4	Management of FAU_STG.2	20
7.6.5	Management of FAU_STG.3	20
7.6.6	Management of FAU_STG.4	20
7.6.7	Audit of FAU_STG.1, FAU_STG.2	20
7.6.8	Audit of FAU_STG.3	20
7.6.9	Audit of FAU_STG.4	21
7.6.10	FAU_STG.1 Protected audit trail storage	21
7.6.11	FAU_STG.2 Guarantees of audit data availability	21
7.6.12	FAU_STG.3 Action in case of possible audit data loss	21
7.6.13	FAU_STG.4 Prevention of audit data loss	21
8	Class FCO: Communication	22
8.1	Non-repudiation of origin (FCO_NRO)	22
8.1.1	Family Behaviour	22
8.1.2	Component levelling	22
8.1.3	Management of FCO_NRO.1, FCO_NRO.2	22
8.1.4	Audit of FCO_NRO.1	22
8.1.5	Audit of FCO_NRO.2	23
8.1.6	FCO_NRO.1 Selective proof of origin	23
8.1.7	FCO_NRO.2 Enforced proof of origin	23
8.2	Non-repudiation of receipt (FCO_NRR)	24
8.2.1	Family Behaviour	24
8.2.2	Component levelling	24
8.2.3	Management of FCO_NRR.1, FCO_NRR.2	24
8.2.4	Audit of FCO_NRR.1	24
8.2.5	Audit of FCO_NRR.2	24
8.2.6	FCO_NRR.1 Selective proof of receipt	24
8.2.7	FCO_NRR.2 Enforced proof of receipt	25
9	Class FCS: Cryptographic support	25
9.1	Cryptographic key management (FCS_CKM)	26
9.1.1	Family Behaviour	26
9.1.2	Component levelling	26
9.1.3	Management of FCS_CKM.1, FCS_CKM.2, FCS_CKM.3, FCS_CKM.4	27
9.1.4	Audit of FCS_CKM.1, FCS_CKM.2, FCS_CKM.3, FCS_CKM.4	27
9.1.5	FCS_CKM.1 Cryptographic key generation	27
9.1.6	FCS_CKM.2 Cryptographic key distribution	27
9.1.7	FCS_CKM.3 Cryptographic key access	27
9.1.8	FCS_CKM.4 Cryptographic key destruction	28
9.2	Cryptographic operation (FCS_COP)	28
9.2.1	Family Behaviour	28
9.2.2	Component levelling	28
9.2.3	Management of FCS_COP.1	28
9.2.4	Audit of FCS_COP.1	29
9.2.5	FCS_COP.1 Cryptographic operation	29
10	Class FDP: User data protection	29

THE STANDARD PREVIEW
 (standards.iteh.ai)
 ISO/IEC 15408-2:2005
<https://standards.iteh.ai/catalog/standards/sist/54792c7c-7a08-481e-ac16-49da780c/iso-iec-15408-2-2005>

10.1	Access control policy (FDP_ACC).....	31
10.1.1	Family Behaviour.....	31
10.1.2	Component levelling	32
10.1.3	Management of FDP_ACC.1, FDP_ACC.2.....	32
10.1.4	Audit of FDP_ACC.1, FDP_ACC.2.....	32
10.1.5	FDP_ACC.1 Subset access control	32
10.1.6	FDP_ACC.2 Complete access control.....	32
10.2	Access control functions (FDP_ACF)	33
10.2.1	Family Behaviour.....	33
10.2.2	Component levelling	33
10.2.3	Management of FDP_ACF.1	33
10.2.4	Audit of FDP_ACF.1	33
10.2.5	FDP_ACF.1 Security attribute based access control	33
10.3	Data authentication (FDP_DAU).....	34
10.3.1	Family Behaviour.....	34
10.3.2	Component levelling	34
10.3.3	Management of FDP_DAU.1, FDP_DAU.2.....	34
10.3.4	Audit of FDP_DAU.1	34
10.3.5	Audit of FDP_DAU.2.....	35
10.3.6	FDP_DAU.1 Basic Data Authentication.....	35
10.3.7	FDP_DAU.2 Data Authentication with Identity of Guarantor	35
10.4	Export to outside TSF control (FDP_ETC).....	35
10.4.1	Family Behaviour.....	35
10.4.2	Component levelling	36
10.4.3	Management of FDP_ETC.1.....	36
10.4.4	Management of FDP_ETC.2.....	36
10.4.5	Audit of FDP_ETC.1, FDP_ETC.2.....	36
10.4.6	FDP_ETC.1 Export of user data without security attributes.....	36
10.4.7	FDP_ETC.2 Export of user data with security attributes.....	36
10.5	Information flow control policy (FDP_IFC)	37
10.5.1	Family Behaviour.....	37
10.5.2	Component levelling.....	37
10.5.3	Management of FDP_IFC.1, FDP_IFC.2.....	38
10.5.4	Audit of FDP_IFC.1, FDP_IFC.2.....	38
10.5.5	FDP_IFC.1 Subset information flow control	38
10.5.6	FDP_IFC.2 Complete information flow control.....	38
10.6	Information flow control functions (FDP_IFF).....	38
10.6.1	Family Behaviour.....	38
10.6.2	Component levelling	38
10.6.3	Management of FDP_IFF.1, FDP_IFF.2.....	39
10.6.4	Management of FDP_IFF.3, FDP_IFF.4, FDP_IFF.5	39
10.6.5	Management of FDP_IFF.6	39
10.6.6	Audit of FDP_IFF.1, FDP_IFF.2, FDP_IFF.5.....	39
10.6.7	Audit of FDP_IFF.3, FDP_IFF.4, FDP_IFF.6.....	39
10.6.8	FDP_IFF.1 Simple security attributes.....	40
10.6.9	FDP_IFF.2 Hierarchical security attributes.....	40
10.6.10	FDP_IFF.3 Limited illicit information flows.....	41
10.6.11	FDP_IFF.4 Partial elimination of illicit information flows.....	42
10.6.12	FDP_IFF.5 No illicit information flows.....	42
10.6.13	FDP_IFF.6 Illicit information flow monitoring.....	42
10.7	Import from outside TSF control (FDP_ITC).....	42
10.7.1	Family Behaviour.....	42
10.7.2	Component levelling	43
10.7.3	Management of FDP_ITC.1, FDP_ITC.2.....	43
10.7.4	Audit of FDP_ITC.1, FDP_ITC.2.....	43
10.7.5	FDP_ITC.1 Import of user data without security attributes.....	43
10.7.6	FDP_ITC.2 Import of user data with security attributes	44
10.8	Internal TOE transfer (FDP_ITT).....	44
10.8.1	Family Behaviour.....	44
10.8.2	Component levelling	44

10.8.3	Management of FDP_ITT.1, FDP_ITT.2	45
10.8.4	Management of FDP_ITT.3, FDP_ITT.4	45
10.8.5	Audit of FDP_ITT.1, FDP_ITT.2	45
10.8.6	Audit of FDP_ITT.3, FDP_ITT.4	45
10.8.7	FDP_ITT.1 Basic internal transfer protection	45
10.8.8	FDP_ITT.2 Transmission separation by attribute	46
10.8.9	FDP_ITT.3 Integrity monitoring	46
10.8.10	FDP_ITT.4 Attribute-based integrity monitoring	46
10.9	Residual information protection (FDP_RIP)	47
10.9.1	Family Behaviour	47
10.9.2	Component levelling	47
10.9.3	Management of FDP_RIP.1, FDP_RIP.2	47
10.9.4	Audit of FDP_RIP.1, FDP_RIP.2	47
10.9.5	FDP_RIP.1 Subset residual information protection	47
10.9.6	FDP_RIP.2 Full residual information protection	48
10.10	Rollback (FDP_ROL)	48
10.10.1	Family Behaviour	48
10.10.2	Component levelling	48
10.10.3	Management of FDP_ROL.1, FDP_ROL.2	48
10.10.4	Audit of FDP_ROL.1, FDP_ROL.2	48
10.10.5	FDP_ROL.1 Basic rollback	48
10.10.6	FDP_ROL.2 Advanced rollback	49
10.11	Stored data integrity (FDP_SDI)	49
10.11.1	Family Behaviour	49
10.11.2	Component levelling	49
10.11.3	Management of FDP_SDI.1	49
10.11.4	Management of FDP_SDI.2	50
10.11.5	Audit of FDP_SDI.1	50
10.11.6	Audit of FDP_SDI.2	50
10.11.7	FDP_SDI.1 Stored data integrity monitoring	50
10.11.8	FDP_SDI.2 Stored data integrity monitoring and action	50
10.12	Inter-TSF user data confidentiality transfer protection (FDP_UCT)	51
10.12.1	Family Behaviour	51
10.12.2	Component levelling	51
10.12.3	Management of FDP_UCT.1	51
10.12.4	Audit of FDP_UCT.1	51
10.12.5	FDP_UCT.1 Basic data exchange confidentiality	51
10.13	Inter-TSF user data integrity transfer protection (FDP_UIT)	51
10.13.1	Family Behaviour	51
10.13.2	Component levelling	52
10.13.3	Management of FDP_UIT.1, FDP_UIT.2, FDP_UIT.3	52
10.13.4	Audit of FDP_UIT.1	52
10.13.5	Audit of FDP_UIT.2, FDP_UIT.3	52
10.13.6	FDP_UIT.1 Data exchange integrity	53
10.13.7	FDP_UIT.2 Source data exchange recovery	53
10.13.8	FDP_UIT.3 Destination data exchange recovery	53
11	Class FIA: Identification and authentication	54
11.1	Authentication failures (FIA_AFL)	54
11.1.1	Family Behaviour	54
11.1.2	Component levelling	55
11.1.3	Management of FIA_AFL.1	55
11.1.4	Audit of FIA_AFL.1	55
11.1.5	FIA_AFL.1 Authentication failure handling	55
11.2	User attribute definition (FIA_ATD)	55
11.2.1	Family Behaviour	55
11.2.2	Component levelling	56
11.2.3	Management of FIA_ATD.1	56
11.2.4	Audit of FIA_ATD.1	56
11.2.5	FIA_ATD.1 User attribute definition	56



 (standards.itech.ai)

ISO/IEC 15408-2:2005

http://standards.itech.ai/standards/preview/15408-2-2005-481c-ac16-571749da786e/iso-iec-15408-2-2005

11.3	Specification of secrets (FIA_SOS)	56
11.3.1	Family Behaviour.....	56
11.3.2	Component levelling	56
11.3.3	Management of FIA_SOS.1.....	56
11.3.4	Management of FIA_SOS.2.....	57
11.3.5	Audit of FIA_SOS.1, FIA_SOS.2.....	57
11.3.6	FIA_SOS.1 Verification of secrets	57
11.3.7	FIA_SOS.2 TSF Generation of secrets	57
11.4	User authentication (FIA_UAU).....	57
11.4.1	Family Behaviour.....	57
11.4.2	Component levelling	58
11.4.3	Management of FIA_UAU.1	58
11.4.4	Management of FIA_UAU.2	58
11.4.5	Management of FIA_UAU.3, FIA_UAU.4, FIA_UAU.7	59
11.4.6	Management of FIA_UAU.5	59
11.4.7	Management of FIA_UAU.6	59
11.4.8	Audit of FIA_UAU.1	59
11.4.9	Audit of FIA_UAU.2	59
11.4.10	Audit of FIA_UAU.3	59
11.4.11	Audit of FIA_UAU.4	59
11.4.12	Audit of FIA_UAU.5	59
11.4.13	Audit of FIA_UAU.6	60
11.4.14	Audit of FIA_UAU.7	60
11.4.15	FIA_UAU.1 Timing of authentication.....	60
11.4.16	FIA_UAU.2 User authentication before any action	60
11.4.17	FIA_UAU.3 Unforgeable authentication.....	60
11.4.18	FIA_UAU.4 Single-use authentication mechanisms.....	61
11.4.19	FIA_UAU.5 Multiple authentication mechanisms.....	61
11.4.20	FIA_UAU.6 Re-authenticating	61
11.4.21	FIA_UAU.7 Protected authentication feedback.....	61
11.5	User identification (FIA_UID).....	61
11.5.1	Family Behaviour.....	61
11.5.2	Component levelling	62
11.5.3	Management of FIA_UID.1	62
11.5.4	Management of FIA_UID.2	62
11.5.5	Audit of FIA_UID.1, FIA_UID.2.....	62
11.5.6	FIA_UID.1 Timing of identification.....	62
11.5.7	FIA_UID.2 User identification before any action	62
11.6	User-subject binding (FIA_USB).....	63
11.6.1	Family Behaviour.....	63
11.6.2	Component levelling	63
11.6.3	Management of FIA_USB.1	63
11.6.4	Audit of FIA_USB.1.....	63
11.6.5	FIA_USB.1 User-subject binding	63
12	Class FMT: Security management.....	64
12.1	Management of functions in TSF (FMT_MOF).....	65
12.1.1	Family Behaviour.....	65
12.1.2	Component levelling	65
12.1.3	Management of FMT_MOF.1	65
12.1.4	Audit of FMT_MOF.1.....	65
12.1.5	FMT_MOF.1 Management of security functions behaviour	65
12.2	Management of security attributes (FMT_MSA).....	65
12.2.1	Family Behaviour.....	65
12.2.2	Component levelling	66
12.2.3	Management of FMT_MSA.1	66
12.2.4	Management of FMT_MSA.2	66
12.2.5	Management of FMT_MSA.3.....	66
12.2.6	Audit of FMT_MSA.1.....	66
12.2.7	Audit of FMT_MSA.2.....	66

12.2.8	Audit of FMT_MSA.3.....	67
12.2.9	FMT_MSA.1 Management of security attributes.....	67
12.2.10	FMT_MSA.2 Secure security attributes	67
12.2.11	FMT_MSA.3 Static attribute initialisation	67
12.3	Management of TSF data (FMT_MTD).....	68
12.3.1	Family Behaviour	68
12.3.2	Component levelling	68
12.3.3	Management of FMT_MTD.1	68
12.3.4	Management of FMT_MTD.2	68
12.3.5	Management of FMT_MTD.3	68
12.3.6	Audit of FMT_MTD.1	68
12.3.7	Audit of FMT_MTD.2	69
12.3.8	Audit of FMT_MTD.3	69
12.3.9	FMT_MTD.1 Management of TSF data.....	69
12.3.10	FMT_MTD.2 Management of limits on TSF data.....	69
12.3.11	FMT_MTD.3 Secure TSF data	69
12.4	Revocation (FMT_REV)	70
12.4.1	Family Behaviour	70
12.4.2	Component levelling	70
12.4.3	Management of FMT_REV.1.....	70
12.4.4	Audit of FMT_REV.1.....	70
12.4.5	FMT_REV.1 Revocation.....	70
12.5	Security attribute expiration (FMT_SAE).....	70
12.5.1	Family Behaviour	70
12.5.2	Component levelling	71
12.5.3	Management of FMT_SAE.1.....	71
12.5.4	Audit of FMT_SAE.1.....	71
12.5.5	FMT_SAE.1 Time-limited authorisation.....	71
12.6	Specification of Management Functions (FMT_SMF).....	71
12.6.1	Family Behaviour	71
12.6.2	Component levelling	72
12.6.3	Management of FMT_SMF.1.....	72
12.6.4	Audit of FMT_SMF.1	72
12.6.5	FMT_SMF.1 Specification of Management Functions.....	72
12.7	Security management roles (FMT_SMR).....	72
12.7.1	Family Behaviour	72
12.7.2	Component levelling	72
12.7.3	Management of FMT_SMR.1	73
12.7.4	Management of FMT_SMR.2.....	73
12.7.5	Management of FMT_SMR.3.....	73
12.7.6	Audit of FMT_SMR.1.....	73
12.7.7	Audit of FMT_SMR.2.....	73
12.7.8	Audit of FMT_SMR.3.....	73
12.7.9	FMT_SMR.1 Security roles.....	73
12.7.10	FMT_SMR.2 Restrictions on security roles.....	74
12.7.11	FMT_SMR.3 Assuming roles	74
13	Class FPR: Privacy	74
13.1	Anonymity (FPR_ANO).....	75
13.1.1	Family Behaviour	75
13.1.2	Component levelling	75
13.1.3	Management of FPR_ANO.1, FPR_ANO.2.....	75
13.1.4	Audit of FPR_ANO.1, FPR_ANO.2.....	75
13.1.5	FPR_ANO.1 Anonymity	75
13.1.6	FPR_ANO.2 Anonymity without soliciting information	75
13.2	Pseudonymity (FPR_PSE)	76
13.2.1	Family Behaviour	76
13.2.2	Component levelling	76
13.2.3	Management of FPR_PSE.1, FPR_PSE.2, FPR_PSE.3.....	76
13.2.4	Audit of FPR_PSE.1, FPR_PSE.2, FPR_PSE.3.....	76

STANDARD PREVIEW
 (standards.itech.ai)
 ISO/IEC 15408-2:2005
<https://standards.itech.ai/catalog/standards/sist/54792c7c-7a68-481c-ac16-571749da786e/iso-iec-15408-2-2005>

13.2.5	FPR_PSE.1 Pseudonymity	76
13.2.6	FPR_PSE.2 Reversible pseudonymity	77
13.2.7	FPR_PSE.3 Alias pseudonymity	77
13.3	Unlinkability (FPR_UNL)	78
13.3.1	Family Behaviour	78
13.3.2	Component levelling	78
13.3.3	Management of FPR_UNL.1	78
13.3.4	Audit of FPR_UNL.1	78
13.3.5	FPR_UNL.1 Unlinkability	78
13.4	Unobservability (FPR_UNO)	78
13.4.1	Family Behaviour	78
13.4.2	Component levelling	79
13.4.3	Management of FPR_UNO.1, FPR_UNO.2	79
13.4.4	Management of FPR_UNO.3	79
13.4.5	Management of FPR_UNO.4	79
13.4.6	Audit of FPR_UNO.1, FPR_UNO.2	79
13.4.7	Audit of FPR_UNO.3	79
13.4.8	Audit of FPR_UNO.4	79
13.4.9	FPR_UNO.1 Unobservability	80
13.4.10	FPR_UNO.2 Allocation of information impacting unobservability	80
13.4.11	FPR_UNO.3 Unobservability without soliciting information	80
13.4.12	FPR_UNO.4 Authorised user observability	80
14	Class FPT: Protection of the TSF	80
14.1	Underlying abstract machine test (FPT_AMT)	83
14.1.1	Family Behaviour	83
14.1.2	Component levelling	83
14.1.3	Management of FPT_AMT.1	83
14.1.4	Audit of FPT_AMT.1	83
14.1.5	FPT_AMT.1 Abstract machine testing	83
14.2	Fail secure (FPT_FLS)	83
14.2.1	Family Behaviour	83
14.2.2	Component levelling	84
14.2.3	Management of FPT_FLS.1	84
14.2.4	Audit of FPT_FLS.1	84
14.2.5	FPT_FLS.1 Failure with preservation of secure state	84
14.3	Availability of exported TSF data (FPT_ITA)	84
14.3.1	Family Behaviour	84
14.3.2	Component levelling	84
14.3.3	Management of FPT_ITA.1	84
14.3.4	Audit of FPT_ITA.1	85
14.3.5	FPT_ITA.1 Inter-TSF availability within a defined availability metric	85
14.4	Confidentiality of exported TSF data (FPT_ITC)	85
14.4.1	Family Behaviour	85
14.4.2	Component levelling	85
14.4.3	Management of FPT_ITC.1	85
14.4.4	Audit of FPT_ITC.1	85
14.4.5	FPT_ITC.1 Inter-TSF confidentiality during transmission	85
14.5	Integrity of exported TSF data (FPT_ITI)	86
14.5.1	Family Behaviour	86
14.5.2	Component levelling	86
14.5.3	Management of FPT_ITI.1	86
14.5.4	Management of FPT_ITI.2	86
14.5.5	Audit of FPT_ITI.1	86
14.5.6	Audit of FPT_ITI.2	86
14.5.7	FPT_ITI.1 Inter-TSF detection of modification	86
14.5.8	FPT_ITI.2 Inter-TSF detection and correction of modification	87
14.6	Internal TOE TSF data transfer (FPT_ITT)	87
14.6.1	Family Behaviour	87
14.6.2	Component levelling	87

14.6.3	Management of FPT_ITT.1	88
14.6.4	Management of FPT_ITT.2	88
14.6.5	Management of FPT_ITT.3	88
14.6.6	Audit of FPT_ITT.1, FPT_ITT.2.....	88
14.6.7	Audit of FPT_ITT.3	88
14.6.8	FPT_ITT.1 Basic internal TSF data transfer protection.....	88
14.6.9	FPT_ITT.2 TSF data transfer separation.....	89
14.6.10	FPT_ITT.3 TSF data integrity monitoring	89
14.7	TSF physical protection (FPT_PHP)	89
14.7.1	Family Behaviour	89
14.7.2	Component levelling	89
14.7.3	Management of FPT_PHP.1	90
14.7.4	Management of FPT_PHP.2	90
14.7.5	Management of FPT_PHP.3	90
14.7.6	Audit of FPT_PHP.1	90
14.7.7	Audit of FPT_PHP.2	90
14.7.8	Audit of FPT_PHP.3	90
14.7.9	FPT_PHP.1 Passive detection of physical attack.....	90
14.7.10	FPT_PHP.2 Notification of physical attack	91
14.7.11	FPT_PHP.3 Resistance to physical attack	91
14.8	Trusted recovery (FPT_RCV).....	91
14.8.1	Family Behaviour	91
14.8.2	Component levelling	91
14.8.3	Management of FPT_RCV.1	92
14.8.4	Management of FPT_RCV.2, FPT_RCV.3	92
14.8.5	Management of FPT_RCV.4	92
14.8.6	Audit of FPT_RCV.1, FPT_RCV.2, FPT_RCV.3.....	92
14.8.7	Audit of FPT_RCV.4.....	92
14.8.8	FPT_RCV.1 Manual recovery	92
14.8.9	FPT_RCV.2 Automated recovery.....	93
14.8.10	FPT_RCV.3 Automated recovery without undue loss.....	93
14.8.11	FPT_RCV.4 Function recovery.....	93
14.9	Replay detection (FPT_RPL).....	94
14.9.1	Family Behaviour	94
14.9.2	Component levelling	94
14.9.3	Management of FPT_RPL.1	94
14.9.4	Audit of FPT_RPL.1	94
14.9.5	FPT_RPL.1 Replay detection.....	94
14.10	Reference mediation (FPT_RVM)	94
14.10.1	Family Behaviour	94
14.10.2	Component levelling	95
14.10.3	Management of FPT_RVM.1.....	95
14.10.4	Audit of FPT_RVM.1	95
14.10.5	FPT_RVM.1 Non-bypassability of the TSP	95
14.11	Domain separation (FPT_SEP).....	95
14.11.1	Family Behaviour	95
14.11.2	Component levelling	96
14.11.3	Management of FPT_SEP.1, FPT_SEP.2, FPT_SEP.3	96
14.11.4	Audit of FPT_SEP.1, FPT_SEP.2, FPT_SEP.3.....	96
14.11.5	FPT_SEP.1 TSF domain separation	96
14.11.6	FPT_SEP.2 SFP domain separation.....	96
14.11.7	FPT_SEP.3 Complete reference monitor.....	97
14.12	State synchrony protocol (FPT_SSP).....	97
14.12.1	Family Behaviour	97
14.12.2	Component levelling	97
14.12.3	Management of FPT_SSP.1, FPT_SSP.2	98
14.12.4	Audit of FPT_SSP.1, FPT_SSP.2	98
14.12.5	FPT_SSP.1 Simple trusted acknowledgement	98
14.12.6	FPT_SSP.2 Mutual trusted acknowledgement.....	98
14.13	Time stamps (FPT_STM).....	98

STANDARD PREVIEW
(standards.itech.ai)

ISO/IEC 15408-2:2005
<http://standards.itech.ai/catalog/standards/sist/54792c7c-7a68-481c-ac16-571749da786e/iso-iec-15408-2-2005>

14.13.1	Family Behaviour.....	98
14.13.2	Component levelling	98
14.13.3	Management of FPT_STM.1	98
14.13.4	Audit of FPT_STM.1	99
14.13.5	FPT_STM.1 Reliable time stamps	99
14.14	Inter-TSF TSF data consistency (FPT_TDC).....	99
14.14.1	Family Behaviour.....	99
14.14.2	Component levelling	99
14.14.3	Management of FPT_TDC.1	99
14.14.4	Audit of FPT_TDC.1	99
14.14.5	FPT_TDC.1 Inter-TSF basic TSF data consistency	100
14.15	Internal TOE TSF data replication consistency (FPT_TRC).....	100
14.15.1	Family Behaviour.....	100
14.15.2	Component levelling	100
14.15.3	Management of FPT_TRC.1	100
14.15.4	Audit of FPT_TRC.1	100
14.15.5	FPT_TRC.1 Internal TSF consistency.....	100
14.16	TSF self test (FPT_TST)	101
14.16.1	Family Behaviour.....	101
14.16.2	Component levelling	101
14.16.3	Management of FPT_TST.1	101
14.16.4	Audit of FPT_TST.1	101
14.16.5	FPT_TST.1 TSF testing	101
15	Class FRU: Resource utilisation.....	102
15.1	Fault tolerance (FRU_FLT).....	102
15.1.1	Family Behaviour.....	102
15.1.2	Component levelling	102
15.1.3	Management of FRU_FLT.1, FRU_FLT.2	103
15.1.4	Audit of FRU_FLT.1	103
15.1.5	Audit of FRU_FLT.2	103
15.1.6	FRU_FLT.1 Degraded fault tolerance.....	103
15.1.7	FRU_FLT.2 Limited fault tolerance.....	103
15.2	Priority of service (FRU_PRS).....	103
15.2.1	Family Behaviour.....	103
15.2.2	Component levelling	103
15.2.3	Management of FRU_PRS.1, FRU_PRS.2	104
15.2.4	Audit of FRU_PRS.1, FRU_PRS.2	104
15.2.5	FRU_PRS.1 Limited priority of service.....	104
15.2.6	FRU_PRS.2 Full priority of service	104
15.3	Resource allocation (FRU_RSA).....	104
15.3.1	Family Behaviour.....	104
15.3.2	Component levelling	105
15.3.3	Management of FRU_RSA.1	105
15.3.4	Management of FRU_RSA.2	105
15.3.5	Audit of FRU_RSA.1, FRU_RSA.2.....	105
15.3.6	FRU_RSA.1 Maximum quotas	105
15.3.7	FRU_RSA.2 Minimum and maximum quotas.....	105
16	Class FTA: TOE access	106
16.1	Limitation on scope of selectable attributes (FTA_LSA)	106
16.1.1	Family Behaviour.....	106
16.1.2	Component levelling	106
16.1.3	Management of FTA_LSA.1	107
16.1.4	Audit of FTA_LSA.1	107
16.1.5	FTA_LSA.1 Limitation on scope of selectable attributes.....	107
16.2	Limitation on multiple concurrent sessions (FTA_MCS).....	107
16.2.1	Family Behaviour.....	107
16.2.2	Component levelling	107
16.2.3	Management of FTA_MCS.1	107
16.2.4	Management of FTA_MCS.2	108

16.2.5	Audit of FTA_MCS.1, FTA_MCS.2	108
16.2.6	FTA_MCS.1 Basic limitation on multiple concurrent sessions	108
16.2.7	FTA_MCS.2 Per user attribute limitation on multiple concurrent sessions	108
16.3	Session locking (FTA_SSL)	108
16.3.1	Family Behaviour	108
16.3.2	Component levelling	109
16.3.3	Management of FTA_SSL.1	109
16.3.4	Management of FTA_SSL.2	109
16.3.5	Management of FTA_SSL.3	109
16.3.6	Audit of FTA_SSL.1, FTA_SSL.2	109
16.3.7	Audit of FTA_SSL.3	110
16.3.8	FTA_SSL.1 TSF-initiated session locking	110
16.3.9	FTA_SSL.2 User-initiated locking	110
16.3.10	FTA_SSL.3 TSF-initiated termination	110
16.4	TOE access banners (FTA_TAB).....	111
16.4.1	Family Behaviour	111
16.4.2	Component levelling	111
16.4.3	Management of FTA_TAB.1	111
16.4.4	Audit of FTA_TAB.1	111
16.4.5	FTA_TAB.1 Default TOE access banners.....	111
16.5	TOE access history (FTA_TAH).....	111
16.5.1	Family Behaviour	111
16.5.2	Component levelling	111
16.5.3	Management of FTA_TAH.1	111
16.5.4	Audit of FTA_TAH.1	112
16.5.5	FTA_TAH.1 TOE access history	112
16.6	TOE session establishment (FTA_TSE)	112
16.6.1	Family Behaviour	112
16.6.2	Component levelling	112
16.6.3	Management of FTA_TSE.1	112
16.6.4	Audit of FTA_TSE.1	112
16.6.5	FTA_TSE.1 TOE session establishment.....	113
17	Class FTP: Trusted path/channels.....	113
17.1	Inter-TSF trusted channel (FTP_ITC)	113
17.1.1	Family Behaviour	113
17.1.2	Component levelling	113
17.1.3	Management of FTP_ITC.1	114
17.1.4	Audit of FTP_ITC.1	114
17.1.5	FTP_ITC.1 Inter-TSF trusted channel.....	114
17.2	Trusted path (FTP_TRP).....	114
17.2.1	Family Behaviour	114
17.2.2	Component levelling	115
17.2.3	Management of FTP_TRP.1	115
17.2.4	Audit of FTP_TRP.1	115
17.2.5	FTP_TRP.1 Trusted path	115
Annex A	(normative) Security functional requirements application notes.....	116
A.1	Structure of the notes	116
A.1.1	Class structure.....	116
A.1.2	Family structure.....	116
A.1.3	Component structure	117
A.2	Dependency tables	118
Annex B	(normative) Functional classes, families, and components	124
Annex C	(normative) Class FAU: Security audit.....	125
C.1	Audit requirements in a distributed environment	125
C.2	Security audit automatic response (FAU_ARP)	126
C.2.1	Application notes.....	126
C.2.2	FAU_ARP.1 Security alarms	126
C.3	Security audit data generation (FAU_GEN)	127

INTERNATIONAL STANDARD PREVIEW
 (standards.itech.ai)
 ISO/IEC 15408-2:2005
<https://standards.itech.ai/catalog/standards/sist/54792c7c-7a68-481c-ac16-571749da786e/iso-iec-15408-2-2005>

C.3.1	Application notes	127
C.3.2	FAU_GEN.1 Audit data generation	128
C.3.3	FAU_GEN.2 User identity association.....	128
C.4	Security audit analysis (FAU_SAA).....	129
C.4.1	Application notes	129
C.4.2	FAU_SAA.1 Potential violation analysis	129
C.4.3	FAU_SAA.2 Profile based anomaly detection	129
C.4.4	FAU_SAA.3 Simple attack heuristics	130
C.4.5	FAU_SAA.4 Complex attack heuristics.....	131
C.5	Security audit review (FAU_SAR).....	132
C.5.1	Application notes	132
C.5.2	FAU_SAR.1 Audit review	133
C.5.3	FAU_SAR.2 Restricted audit review	133
C.5.4	FAU_SAR.3 Selectable audit review	133
C.6	Security audit event selection (FAU_SEL).....	134
C.6.1	Application notes	134
C.6.2	FAU_SEL.1 Selective audit.....	134
C.7	Security audit event storage (FAU_STG).....	134
C.7.1	Application notes	134
C.7.2	FAU_STG.1 Protected audit trail storage.....	134
C.7.3	FAU_STG.2 Guarantees of audit data availability.....	135
C.7.4	FAU_STG.3 Action in case of possible audit data loss.....	135
C.7.5	FAU_STG.4 Prevention of audit data loss	136
Annex D	(normative) Class FCO: Communication.....	137
D.1	Non-repudiation of origin (FCO_NRO)	137
D.1.1	User notes	137
D.1.2	FCO_NRO.1 Selective proof of origin.....	138
D.1.3	FCO_NRO.2 Enforced proof of origin.....	138
D.2	Non-repudiation of receipt (FCO_NRR).....	139
D.2.1	User notes	139
D.2.2	FCO_NRR.1 Selective proof of receipt.....	139
D.2.3	FCO_NRR.2 Enforced proof of receipt.....	140
Annex E	(normative) Class FCS: Cryptographic support.....	141
E.1	Cryptographic key management (FCS_CKM).....	142
E.1.1	User notes	142
E.1.2	FCS_CKM.1 Cryptographic key generation.....	142
E.1.3	FCS_CKM.2 Cryptographic key distribution.....	143
E.1.4	FCS_CKM.3 Cryptographic key access	143
E.1.5	FCS_CKM.4 Cryptographic key destruction.....	143
E.2	Cryptographic operation (FCS_COP).....	144
E.2.1	User notes	144
E.2.2	FCS_COP.1 Cryptographic operation	144
Annex F	(normative) Class FDP: User data protection.....	146
F.1	Access control policy (FDP_ACC).....	149
F.1.1	User notes	149
F.1.2	FDP_ACC.1 Subset access control	149
F.1.3	FDP_ACC.2 Complete access control.....	150
F.2	Access control functions (FDP_ACF)	150
F.2.1	User notes	150
F.2.2	FDP_ACF.1 Security attribute based access control	150
F.3	Data authentication (FDP_DAU).....	152
F.3.1	User notes	152
F.3.2	FDP_DAU.1 Basic Data Authentication.....	152
F.3.3	FDP_DAU.2 Data Authentication with Identity of Guarantor	152
F.4	Export to outside TSF control (FDP_ETC).....	152
F.4.1	User notes	152
F.4.2	FDP_ETC.1 Export of user data without security attributes	153
F.4.3	FDP_ETC.2 Export of user data with security attributes.....	153

F.5	Information flow control policy (FDP_IFC).....	154
F.5.1	User notes	154
F.5.2	FDP_IFC.1 Subset information flow control	155
F.5.3	FDP_IFC.2 Complete information flow control	155
F.6	Information flow control functions (FDP_IFF)	155
F.6.1	User notes	155
F.6.2	FDP_IFF.1 Simple security attributes	156
F.6.3	FDP_IFF.2 Hierarchical security attributes	157
F.6.4	FDP_IFF.3 Limited illicit information flows	158
F.6.5	FDP_IFF.4 Partial elimination of illicit information flows	158
F.6.6	FDP_IFF.5 No illicit information flows	159
F.6.7	FDP_IFF.6 Illicit information flow monitoring	159
F.7	Import from outside TSF control (FDP_ITC)	159
F.7.1	User notes	159
F.7.2	FDP_ITC.1 Import of user data without security attributes	160
F.7.3	FDP_ITC.2 Import of user data with security attributes	161
F.8	Internal TOE transfer (FDP_ITT)	161
F.8.1	User notes	161
F.8.2	FDP_ITT.1 Basic internal transfer protection	162
F.8.3	FDP_ITT.2 Transmission separation by attribute	162
F.8.4	FDP_ITT.3 Integrity monitoring	162
F.8.5	FDP_ITT.4 Attribute-based integrity monitoring	163
F.9	Residual information protection (FDP_RIP)	164
F.9.1	User notes	164
F.9.2	FDP_RIP.1 Subset residual information protection	164
F.9.3	FDP_RIP.2 Full residual information protection	165
F.10	Rollback (FDP_ROL)	165
F.10.1	User notes	165
F.10.2	FDP_ROL.1 Basic rollback	165
F.10.3	FDP_ROL.2 Advanced rollback	166
F.11	Stored data integrity (FDP_SDI)	166
F.11.1	User notes	166
F.11.2	FDP_SDI.1 Stored data integrity monitoring	167
F.11.3	FDP_SDI.2 Stored data integrity monitoring and action	167
F.12	Inter-TSF user data confidentiality transfer protection (FDP_UCT)	167
F.12.1	User notes	167
F.12.2	FDP_UCT.1 Basic data exchange confidentiality	167
F.13	Inter-TSF user data integrity transfer protection (FDP_UIT)	168
F.13.1	User notes	168
F.13.2	FDP_UIT.1 Data exchange integrity	168
F.13.3	FDP_UIT.2 Source data exchange recovery	169
F.13.4	FDP_UIT.3 Destination data exchange recovery	169
Annex G	(normative) Class FIA: Identification and authentication	170
G.1	Authentication failures (FIA_AFL)	171
G.1.1	User notes	171
G.1.2	FIA_AFL.1 Authentication failure handling	171
G.2	User attribute definition (FIA_ATD)	172
G.2.1	User notes	172
G.2.2	FIA_ATD.1 User attribute definition	173
G.3	Specification of secrets (FIA_SOS)	173
G.3.1	User notes	173
G.3.2	FIA_SOS.1 Verification of secrets	173
G.3.3	FIA_SOS.2 TSF Generation of secrets	174
G.4	User authentication (FIA_UAU)	174
G.4.1	User notes	174
G.4.2	FIA_UAU.1 Timing of authentication	174
G.4.3	FIA_UAU.2 User authentication before any action	175
G.4.4	FIA_UAU.3 Unforgeable authentication	175
G.4.5	FIA_UAU.4 Single-use authentication mechanisms	175

G.4.6	FIA_UAU.5 Multiple authentication mechanisms.....	175
G.4.7	FIA_UAU.6 Re-authenticating	176
G.4.8	FIA_UAU.7 Protected authentication feedback.....	176
G.5	User identification (FIA_UID).....	177
G.5.1	User notes	177
G.5.2	FIA_UID.1 Timing of identification.....	177
G.5.3	FIA_UID.2 User identification before any action	177
G.6	User-subject binding (FIA_USB).....	177
G.6.1	User notes	177
G.6.2	FIA_USB.1 User-subject binding	177
Annex H	(normative) Class FMT: Security management.....	179
H.1	Management of functions in TSF (FMT_MOF).....	180
H.1.1	User notes	180
H.1.2	FMT_MOF.1 Management of security functions behaviour	180
H.2	Management of security attributes (FMT_MSA).....	181
H.2.1	User notes	181
H.2.2	FMT_MSA.1 Management of security attributes	181
H.2.3	FMT_MSA.2 Secure security attributes.....	182
H.2.4	FMT_MSA.3 Static attribute initialisation.....	182
H.3	Management of TSF data (FMT_MTD).....	182
H.3.1	User notes	182
H.3.2	FMT_MTD.1 Management of TSF data.....	182
H.3.3	FMT_MTD.2 Management of limits on TSF data.....	183
H.3.4	FMT_MTD.3 Secure TSF data	183
H.4	Revocation (FMT_REV).....	184
H.4.1	User notes	184
H.4.2	FMT_REV.1 Revocation	184
H.5	Security attribute expiration (FMT_SAE).....	184
H.5.1	User notes	184
H.5.2	FMT_SAE.1 Time-limited authorisation.....	184
H.6	Specification of Management Functions (FMT_SMF).....	185
H.6.1	User notes	185
H.6.2	FMT_SMF.1 Specification of Management Functions	185
H.7	Security management roles (FMT_SMR).....	185
H.7.1	User notes	185
H.7.2	FMT_SMR.1 Security roles	186
H.7.3	FMT_SMR.2 Restrictions on security roles	186
H.7.4	FMT_SMR.3 Assuming roles	186
Annex I	(normative) Class FPR: Privacy	187
I.1	Anonymity (FPR_ANO)	188
I.1.1	User notes	188
I.1.2	FPR_ANO.1 Anonymity.....	189
I.1.3	FPR_ANO.2 Anonymity without soliciting information.....	189
I.2	Pseudonymity (FPR_PSE).....	189
I.2.1	User notes	189
I.2.2	FPR_PSE.1 Pseudonymity	190
I.2.3	FPR_PSE.2 Reversible pseudonymity	191
I.2.4	FPR_PSE.3 Alias pseudonymity	192
I.3	Unlinkability (FPR_UNL).....	193
I.3.1	User notes	193
I.3.2	FPR_UNL.1 Unlinkability.....	193
I.4	Unobservability (FPR_UNO).....	194
I.4.1	User notes	194
I.4.2	FPR_UNO.1 Unobservability	195
I.4.3	FPR_UNO.2 Allocation of information impacting unobservability.....	195
I.4.4	FPR_UNO.3 Unobservability without soliciting information.....	196
I.4.5	FPR_UNO.4 Authorised user observability	197