



**International  
Standard**

**ISO/IEC 15408-2**

**Information security, cybersecurity  
and privacy protection —  
Evaluation criteria for IT security —**

**Part 2:  
Security functional components**

*Sécurité de l'information, cybersécurité et protection de la vie  
privée — Critères d'évaluation pour la sécurité des technologies  
de l'information —*

*Partie 2: Composants fonctionnels de sécurité*

**Fifth edition  
2026-05**



**COPYRIGHT PROTECTED DOCUMENT**

© ISO/IEC 2026

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office  
CP 401 • Ch. de Blandonnet 8  
CH-1214 Vernier, Geneva  
Phone: +41 22 749 01 11  
Email: [copyright@iso.org](mailto:copyright@iso.org)  
Website: [www.iso.org](http://www.iso.org)

Published in Switzerland

# Contents

	Page
<b>Foreword</b> .....	<b>xv</b>
<b>Introduction</b> .....	<b>xvi</b>
<b>1 Scope</b> .....	<b>1</b>
<b>2 Normative references</b> .....	<b>1</b>
<b>3 Terms and definitions</b> .....	<b>1</b>
<b>4 Abbreviated terms</b> .....	<b>3</b>
<b>5 Overview</b> .....	<b>4</b>
5.1 General.....	4
5.2 Organization of this document.....	4
<b>6 Functional requirements paradigm</b> .....	<b>5</b>
<b>7 Security functional components</b> .....	<b>8</b>
7.1 Overview.....	8
7.2 Functional class structure.....	8
7.2.1 General.....	8
7.2.2 Class name.....	9
7.2.3 Class introduction.....	9
7.2.4 Class informative notes.....	9
7.2.5 Functional families.....	9
7.3 Functional family structure.....	9
7.3.1 General.....	9
7.3.2 Family name.....	10
7.3.3 Family Behaviour.....	10
7.3.4 Component levelling and description.....	10
7.3.5 Component management.....	10
7.3.6 Component audit.....	11
7.3.7 Family application notes.....	11
7.3.8 Family evaluator notes.....	11
7.3.9 Functional components.....	11
7.4 Functional component structure.....	12
7.4.1 General.....	12
7.4.2 Component name.....	12
7.4.3 Component relationships.....	12
7.4.4 Component rationale.....	13
7.4.5 Component notes.....	13
7.4.6 Functional elements.....	13
7.5 Functional elements.....	13
7.6 Component catalogue.....	14
7.6.1 General.....	14
7.6.2 Highlighting of component changes.....	15
<b>8 Class FAU Security audit</b> .....	<b>15</b>
8.1 Introduction.....	15
8.2 Notes on class FAU.....	17
8.2.1 General information about audit requirements.....	17
8.2.2 Audit requirements in a distributed environment.....	17
8.3 Security audit automatic response (FAU_ARP).....	18
8.3.1 Family Behaviour.....	18
8.3.2 Component levelling and description.....	18
8.3.3 Component management.....	18
8.3.4 Component audit.....	18
8.3.5 Application notes.....	18
8.3.6 FAU_ARP.1 Security alarms.....	19
8.4 Security audit data generation (FAU_GEN).....	19

## ISO/IEC 15408-2:2026(en)

	8.4.1 Family Behaviour.....	19
	8.4.2 Component levelling and description.....	19
	8.4.3 Component management.....	19
	8.4.4 Component audit.....	20
	8.4.5 Application notes.....	20
	8.4.6 Evaluator notes.....	21
	8.4.7 FAU_GEN.1 Audit data generation.....	21
	8.4.8 FAU_GEN.2 User identity association.....	22
8.5	Security audit analysis (FAU_SAA).....	23
	8.5.1 Family Behaviour.....	23
	8.5.2 Component levelling and description.....	23
	8.5.3 Component management.....	23
	8.5.4 Component audit.....	24
	8.5.5 Application notes.....	24
	8.5.6 FAU_SAA.1 Potential violation analysis.....	24
	8.5.7 FAU_SAA.2 Profile based anomaly detection.....	25
	8.5.8 FAU_SAA.3 Simple attack heuristics.....	26
	8.5.9 FAU_SAA.4 Complex attack heuristics.....	27
8.6	Security audit review (FAU_SAR).....	29
	8.6.1 Family Behaviour.....	29
	8.6.2 Component levelling and description.....	29
	8.6.3 Component management.....	29
	8.6.4 Component audit.....	30
	8.6.5 Application notes.....	30
	8.6.6 FAU_SAR.1 Audit review.....	30
	8.6.7 FAU_SAR.2 Restricted audit review.....	31
	8.6.8 FAU_SAR.3 Selectable audit review.....	31
8.7	Security audit event selection (FAU_SEL).....	32
	8.7.1 Family Behaviour.....	32
	8.7.2 Component levelling and description.....	32
	8.7.3 Component management.....	32
	8.7.4 Component audit.....	32
	8.7.5 Application notes.....	32
	8.7.6 FAU_SEL.1 Selective audit.....	33
8.8	Security audit data storage (FAU_STG).....	33
	8.8.1 Family Behaviour.....	33
	8.8.2 Component levelling and description.....	33
	8.8.3 Component management.....	34
	8.8.4 Component audit.....	35
	8.8.5 Application notes.....	35
	8.8.6 FAU_STG.1 Audit data storage location.....	35
	8.8.7 FAU_STG.2 Protected audit data storage.....	36
	8.8.8 FAU_STG.3 Guarantees of audit data availability.....	36
	8.8.9 FAU_STG.4 Action in case of possible audit data loss.....	37
	8.8.10 FAU_STG.5 Prevention of audit data loss.....	38
<b>9</b>	<b>Class FCO Communication.....</b>	<b>38</b>
	9.1 Introduction.....	38
	9.2 Notes on class FCO.....	39
	9.3 Non-repudiation of origin (FCO_NRO).....	39
	9.3.1 Family Behaviour.....	39
	9.3.2 Component levelling and description.....	39
	9.3.3 Component management.....	40
	9.3.4 Component audit.....	40
	9.3.5 Application notes.....	40
	9.3.6 FCO_NRO.1 Selective proof of origin.....	41
	9.3.7 FCO_NRO.2 Enforced proof of origin.....	42
	9.4 Non-repudiation of receipt (FCO_NRR).....	42
	9.4.1 Family Behaviour.....	42

## ISO/IEC 15408-2:2026(en)

9.4.2	Component levelling and description	43
9.4.3	Component management	43
9.4.4	Component audit	43
9.4.5	Application notes	43
9.4.6	FCO_NRR.1 Selective proof of receipt	44
9.4.7	FCO_NRR.2 Enforced proof of receipt	45
<b>10</b>	<b>Class FCS Cryptographic support</b>	<b>46</b>
10.1	Introduction	46
10.2	Notes on class FCS	48
10.3	Cryptographic key management (FCS_CKM)	50
10.3.1	Family Behaviour	50
10.3.2	Component levelling and description	50
10.3.3	Component management	51
10.3.4	Component audit	51
10.3.5	Application notes	51
10.3.6	Evaluator notes	52
10.3.7	FCS_CKM.1 Cryptographic key generation	52
10.3.8	FCS_CKM.2 Cryptographic key distribution	53
10.3.9	FCS_CKM.3 Cryptographic key access	53
10.3.10	FCS_CKM.5 Cryptographic key derivation	54
10.3.11	FCS_CKM.6 Timing and event of cryptographic key destruction	55
10.4	Cryptographic operation (FCS_COP)	56
10.4.1	Family Behaviour	56
10.4.2	Component levelling and description	56
10.4.3	Component management	56
10.4.4	Component audit	56
10.4.5	Application notes	56
10.4.6	FCS_COP.1 Cryptographic operation	57
10.5	Random bit generation (FCS_RBG)	58
10.5.1	Family Behaviour	58
10.5.2	Component levelling and description	58
10.5.3	Component management	59
10.5.4	Component audit	59
10.5.5	Application notes	59
10.5.6	FCS_RBG.1 Random bit generation (RBG)	59
10.5.7	FCS_RBG.2 Random bit generation (external seeding)	61
10.5.8	FCS_RBG.3 Random bit generation (internal seeding - single source)	61
10.5.9	FCS_RBG.4 Random bit generation (internal seeding - multiple sources)	62
10.5.10	FCS_RBG.5 Random bit generation (combining entropy sources)	62
10.5.11	FCS_RBG.6 Random bit generation service	63
10.6	Generation of random numbers (FCS_RNG)	63
10.6.1	Family Behaviour	63
10.6.2	Component levelling and description	64
10.6.3	Component management	64
10.6.4	Component audit	64
10.6.5	Application notes	64
10.6.6	FCS_RNG.1 Random number generation	64
<b>11</b>	<b>Class FDP User data protection</b>	<b>66</b>
11.1	Introduction	66
11.2	Notes on class FDP	69
11.3	Access control policy (FDP_ACC)	71
11.3.1	Family Behaviour	71
11.3.2	Component levelling and description	72
11.3.3	Component management	72
11.3.4	Component audit	72
11.3.5	Application notes	72
11.3.6	FDP_ACC.1 Subset access control	73
11.3.7	FDP_ACC.2 Complete access control	73

## ISO/IEC 15408-2:2026(en)

11.4	Access control functions (FDP_ACF)	74
11.4.1	Family Behaviour	74
11.4.2	Component levelling and description	74
11.4.3	Component management	74
11.4.4	Component audit	75
11.4.5	Application notes	75
11.4.6	FDP_ACF.1 Security attribute-based access control	75
11.5	Data authentication (FDP_DAU)	77
11.5.1	Family Behaviour	77
11.5.2	Component levelling and description	77
11.5.3	Component management	77
11.5.4	Component audit	77
11.5.5	Application notes	78
11.5.6	FDP_DAU.1 Basic Data Authentication	78
11.5.7	FDP_DAU.2 Data Authentication with Identity of Guarantor	78
11.6	Export from the TOE (FDP_ETC)	79
11.6.1	Family Behaviour	79
11.6.2	Component levelling and description	79
11.6.3	Component management	80
11.6.4	Component audit	80
11.6.5	Application notes	80
11.6.6	FDP_ETC.1 Export of user data without security attributes	80
11.6.7	FDP_ETC.2 Export of user data with security attributes	81
11.7	Information flow control policy (FDP_IFC)	82
11.7.1	Family Behaviour	82
11.7.2	Component levelling and description	82
11.7.3	Component management	82
11.7.4	Component audit	82
11.7.5	Application notes	82
11.7.6	FDP_IFC.1 Subset information flow control	83
11.7.7	FDP_IFC.2 Complete information flow control	84
11.8	Information flow control functions (FDP_IFF)	85
11.8.1	Family Behaviour	85
11.8.2	Component levelling and description	85
11.8.3	Component management	86
11.8.4	Component audit	86
11.8.5	Application notes	86
11.8.6	FDP_IFF.1 Simple security attributes	87
11.8.7	FDP_IFF.2 Hierarchical security attributes	88
11.8.8	FDP_IFF.3 Limited illicit information flows	90
11.8.9	FDP_IFF.4 Partial elimination of illicit information flows	91
11.8.10	FDP_IFF.5 No illicit information flows	91
11.8.11	FDP_IFF.6 Illicit information flow monitoring	92
11.9	Information retention control (FDP_IRC)	92
11.9.1	Family Behaviour	92
11.9.2	Component levelling and description	93
11.9.3	Component management	93
11.9.4	Component audit	93
11.9.5	Application notes	93
11.9.6	FDP_IRC.1 Information retention control	94
11.10	Import from outside of the TOE (FDP_ITC)	94
11.10.1	Family Behaviour	94
11.10.2	Component levelling and description	94
11.10.3	Component management	95
11.10.4	Component audit	95
11.10.5	Application notes	95
11.10.6	FDP_ITC.1 Import of user data without security attributes	96
11.10.7	FDP_ITC.2 Import of user data with security attributes	97
11.11	Internal TOE transfer (FDP_ITT)	98

## ISO/IEC 15408-2:2026(en)

11.11.1	Family Behaviour	98
11.11.2	Component levelling and description	98
11.11.3	Component management	98
11.11.4	Component audit	99
11.11.5	Application notes	99
11.11.6	FDP_ITT.1 Basic internal transfer protection	99
11.11.7	FDP_ITT.2 Transmission separation by attribute	100
11.11.8	FDP_ITT.3 Integrity monitoring	101
11.11.9	FDP_ITT.4 Attribute-based integrity monitoring	101
11.12	Residual information protection (FDP_RIP)	102
11.12.1	Family Behaviour	102
11.12.2	Component levelling and description	103
11.12.3	Component management	103
11.12.4	Component audit	103
11.12.5	Application notes	103
11.12.6	FDP_RIP.1 Subset residual information protection	104
11.12.7	FDP_RIP.2 Full residual information protection	105
11.13	Rollback (FDP_ROL)	105
11.13.1	Family Behaviour	105
11.13.2	Component levelling and description	105
11.13.3	Component management	105
11.13.4	Component audit	106
11.13.5	Application notes	106
11.13.6	FDP_ROL.1 Basic rollback	106
11.13.7	FDP_ROL.2 Advanced rollback	107
11.14	Stored data confidentiality (FDP_SDC)	108
11.14.1	Family Behaviour	108
11.14.2	Component levelling and description	108
11.14.3	Component management	108
11.14.4	Component audit	108
11.14.5	Application notes	108
11.14.6	Evaluator notes	108
11.14.7	FDP_SDC.1 Stored data confidentiality	109
11.14.8	FDP_SDC.2 Stored data confidentiality with dedicated method	109
11.15	Stored data integrity (FDP_SDI)	110
11.15.1	Family Behaviour	110
11.15.2	Component levelling and description	110
11.15.3	Component management	110
11.15.4	Component audit	110
11.15.5	Application notes	111
11.15.6	FDP_SDI.1 Stored data integrity monitoring	111
11.15.7	FDP_SDI.2 Stored data integrity monitoring and action	111
11.16	Inter-TSF user data confidentiality transfer protection (FDP_UCT)	112
11.16.1	Family Behaviour	112
11.16.2	Component levelling and description	112
11.16.3	Component management	112
11.16.4	Component audit	112
11.16.5	Application notes	113
11.16.6	FDP_UCT.1 Basic data exchange confidentiality	113
11.17	Inter-TSF user data integrity transfer protection (FDP_UIT)	113
11.17.1	Family Behaviour	113
11.17.2	Component levelling and description	113
11.17.3	Component management	114
11.17.4	Component audit	114
11.17.5	Application notes	115
11.17.6	FDP_UIT.1 Data exchange integrity	115
11.17.7	FDP_UIT.2 Source data exchange recovery	116
11.17.8	FDP_UIT.3 Destination data exchange recovery	116

<b>12</b>	<b>Class FIA Identification and authentication</b>	<b>117</b>
12.1	Introduction	117
12.2	Notes on class FIA	119
12.3	Authentication failures (FIA_AFL)	120
12.3.1	Family Behaviour	120
12.3.2	Component levelling and description	120
12.3.3	Component management	120
12.3.4	Component audit	120
12.3.5	Application notes	120
12.3.6	FIA_AFL.1 Authentication failure handling	121
12.4	Authentication proof of identity (FIA_API)	122
12.4.1	Family Behaviour	122
12.4.2	Component levelling and description	122
12.4.3	Component management	122
12.4.4	Component audit	122
12.4.5	Application notes	122
12.4.6	FIA_API.1 Authentication proof of identity	123
12.5	User attribute definition (FIA_ATD)	123
12.5.1	Family Behaviour	123
12.5.2	Component levelling and description	123
12.5.3	Component management	124
12.5.4	Component audit	124
12.5.5	Application notes	124
12.5.6	FIA_ATD.1 User attribute definition	124
12.6	Specification of secrets (FIA_SOS)	124
12.6.1	Family Behaviour	124
12.6.2	Component levelling and description	124
12.6.3	Component management	125
12.6.4	Component audit	125
12.6.5	Application notes	125
12.6.6	FIA_SOS.1 Verification of secrets	126
12.6.7	FIA_SOS.2 TSF Generation of secrets	126
12.7	User authentication (FIA_UAU)	127
12.7.1	Family Behaviour	127
12.7.2	Component levelling and description	127
12.7.3	Component management	128
12.7.4	Component audit	128
12.7.5	Application notes	129
12.7.6	FIA_UAU.1 Timing of authentication	129
12.7.7	FIA_UAU.2 User authentication before any action	130
12.7.8	FIA_UAU.3 Unforgeable authentication	130
12.7.9	FIA_UAU.4 Single-use authentication mechanisms	131
12.7.10	FIA_UAU.5 Multiple authentication mechanisms	131
12.7.11	FIA_UAU.6 Re-authenticating	132
12.7.12	FIA_UAU.7 Protected authentication feedback	132
12.8	User identification (FIA_UID)	133
12.8.1	Family Behaviour	133
12.8.2	Component levelling and description	133
12.8.3	Component management	133
12.8.4	Component audit	133
12.8.5	Application notes	133
12.8.6	FIA_UID.1 Timing of identification	134
12.8.7	FIA_UID.2 User identification before any action	134
12.9	User-subject binding (FIA_USB)	134
12.9.1	Family Behaviour	134
12.9.2	Component levelling and description	135
12.9.3	Component management	135
12.9.4	Component audit	135
12.9.5	Application notes	135

	12.9.6	FIA_USB.1 User-subject binding.....	135
<b>13</b>		<b>Class FMT Security management.....</b>	<b>136</b>
	13.1	Introduction.....	136
	13.2	Notes on class FMT.....	138
	13.3	Limited capabilities and availability (FMT_LIM).....	138
	13.3.1	Family Behaviour.....	138
	13.3.2	Component levelling and description.....	139
	13.3.3	Component management.....	139
	13.3.4	Component audit.....	139
	13.3.5	Application notes.....	139
	13.3.6	FMT_LIM.1 Limited capabilities.....	139
	13.3.7	FMT_LIM.2 Limited availability.....	140
	13.4	Management of functions in TSF (FMT_MOF).....	140
	13.4.1	Family Behaviour.....	140
	13.4.2	Component levelling and description.....	140
	13.4.3	Component management.....	141
	13.4.4	Component audit.....	141
	13.4.5	Application notes.....	141
	13.4.6	FMT_MOF.1 Management of security functions behaviour.....	142
	13.5	Management of security attributes (FMT_MSA).....	142
	13.5.1	Family Behaviour.....	142
	13.5.2	Component levelling and description.....	142
	13.5.3	Component management.....	143
	13.5.4	Component audit.....	144
	13.5.5	Application notes.....	144
	13.5.6	FMT_MSA.1 Management of security attributes.....	144
	13.5.7	FMT_MSA.2 Secure security attributes.....	145
	13.5.8	FMT_MSA.3 Static attribute initialization.....	146
	13.5.9	FMT_MSA.4 Security attribute value inheritance.....	146
	13.6	Management of TSF data (FMT_MTD).....	147
	13.6.1	Family Behaviour.....	147
	13.6.2	Component levelling and description.....	147
	13.6.3	Component management.....	147
	13.6.4	Component audit.....	148
	13.6.5	Application notes.....	148
	13.6.6	FMT_MTD.1 Management of TSF data.....	148
	13.6.7	FMT_MTD.2 Management of limits on TSF data.....	149
	13.6.8	FMT_MTD.3 Secure TSF data.....	149
	13.7	Revocation (FMT_REV).....	150
	13.7.1	Family Behaviour.....	150
	13.7.2	Component levelling and description.....	150
	13.7.3	Component management.....	150
	13.7.4	Component audit.....	150
	13.7.5	Application notes.....	150
	13.7.6	FMT_REV.1 Revocation.....	150
	13.8	Security attribute expiration (FMT_SAE).....	151
	13.8.1	Family Behaviour.....	151
	13.8.2	Component levelling and description.....	151
	13.8.3	Component management.....	152
	13.8.4	Component audit.....	152
	13.8.5	Application notes.....	152
	13.8.6	FMT_SAE.1 Time-limited authorization.....	152
	13.9	Specification of Management Functions (FMT_SMF).....	153
	13.9.1	Family Behaviour.....	153
	13.9.2	Component levelling and description.....	153
	13.9.3	Component management.....	153
	13.9.4	Component audit.....	153
	13.9.5	Application notes.....	153

## ISO/IEC 15408-2:2026(en)

	13.9.6 FMT_SMF.1 Specification of Management Functions.....	153
13.10	Security management roles (FMT_SMR).....	154
	13.10.1 Family Behaviour.....	154
	13.10.2 Component levelling and description.....	154
	13.10.3 Component management.....	154
	13.10.4 Component audit.....	155
	13.10.5 Application notes.....	155
	13.10.6 FMT_SMR.1 Security roles.....	155
	13.10.7 FMT_SMR.2 Restrictions on security roles.....	156
	13.10.8 FMT_SMR.3 Assuming roles.....	157
<b>14</b>	<b>Class FPR Privacy.....</b>	<b>157</b>
14.1	Introduction.....	157
14.2	Notes on class FPR.....	158
14.3	Anonymity (FPR_ANO).....	159
	14.3.1 Family Behaviour.....	159
	14.3.2 Component levelling and description.....	159
	14.3.3 Component management.....	159
	14.3.4 Component audit.....	159
	14.3.5 Application notes.....	159
	14.3.6 FPR_ANO.1 Anonymity.....	160
	14.3.7 FPR_ANO.2 Anonymity without soliciting information.....	161
14.4	Pseudonymity (FPR_PSE).....	161
	14.4.1 Family Behaviour.....	161
	14.4.2 Component levelling and description.....	161
	14.4.3 Component management.....	162
	14.4.4 Component audit.....	162
	14.4.5 Application notes.....	162
	14.4.6 FPR_PSE.1 Pseudonymity.....	163
	14.4.7 FPR_PSE.2 Reversible pseudonymity.....	164
	14.4.8 FPR_PSE.3 Alias pseudonymity.....	165
14.5	Unlinkability (FPR_UNL).....	167
	14.5.1 Family Behaviour.....	167
	14.5.2 Component levelling and description.....	167
	14.5.3 Component management.....	167
	14.5.4 Component audit.....	167
	14.5.5 Application notes.....	167
	14.5.6 FPR_UNL.1 Unlinkability of operations.....	168
14.6	Unobservability (FPR_UNO).....	169
	14.6.1 Family Behaviour.....	169
	14.6.2 Component levelling and description.....	169
	14.6.3 Component management.....	169
	14.6.4 Component audit.....	169
	14.6.5 Application notes.....	170
	14.6.6 FPR_UNO.1 Unobservability.....	170
	14.6.7 FPR_UNO.2 Allocation of information impacting unobservability.....	171
	14.6.8 FPR_UNO.3 Unobservability without soliciting information.....	172
	14.6.9 FPR_UNO.4 Authorized user observability.....	173
<b>15</b>	<b>Class FPT Protection of the TSF.....</b>	<b>173</b>
15.1	Introduction.....	173
15.2	Notes on class FPT.....	176
15.3	TOE emanation (FPT_EMS).....	177
	15.3.1 Family Behaviour.....	177
	15.3.2 Component levelling and description.....	177
	15.3.3 Component management.....	177
	15.3.4 Component audit.....	178
	15.3.5 Application notes.....	178
	15.3.6 FPT_EMS.1 Emanation of TSF and User data.....	178
15.4	Fail secure (FPT_FLS).....	179

## ISO/IEC 15408-2:2026(en)

15.4.1	Family Behaviour	179
15.4.2	Component levelling and description	179
15.4.3	Component management	179
15.4.4	Component audit	179
15.4.5	Application notes	179
15.4.6	FPT_FLS.1 Failure with preservation of secure state	179
15.5	TSF initialization (FPT_INI)	180
15.5.1	Family Behaviour	180
15.5.2	Component levelling and description	180
15.5.3	Component management	180
15.5.4	Component audit	180
15.5.5	Application notes	180
15.5.6	FPT_INI.1 TSF initialization	181
15.6	Availability of exported TSF data (FPT_ITA)	182
15.6.1	Family Behaviour	182
15.6.2	Component levelling and description	182
15.6.3	Component management	182
15.6.4	Component audit	182
15.6.5	Application notes	182
15.6.6	FPT_ITA.1 Inter-TSF availability within a defined availability metric	182
15.7	Confidentiality of exported TSF data (FPT_ITC)	183
15.7.1	Family Behaviour	183
15.7.2	Component levelling and description	183
15.7.3	Component management	183
15.7.4	Component audit	183
15.7.5	Application notes	183
15.7.6	Evaluator notes	184
15.7.7	FPT_ITC.1 Inter-TSF confidentiality during transmission	184
15.8	Integrity of exported TSF data (FPT_ITI)	184
15.8.1	Family Behaviour	184
15.8.2	Component levelling and description	184
15.8.3	Component management	184
15.8.4	Component audit	185
15.8.5	Application notes	185
15.8.6	Evaluator notes	185
15.8.7	FPT_ITI.1 Inter-TSF detection of modification	185
15.8.8	FPT_ITI.2 Inter-TSF detection and correction of modification	186
15.9	Internal TOE TSF data transfer (FPT_ITT)	187
15.9.1	Family Behaviour	187
15.9.2	Component levelling and description	187
15.9.3	Component management	187
15.9.4	Component audit	188
15.9.5	Application notes	188
15.9.6	Evaluator notes	188
15.9.7	FPT_ITT.1 Basic internal TSF data transfer protection	188
15.9.8	FPT_ITT.2 TSF data transfer separation	189
15.9.9	FPT_ITT.3 TSF data integrity monitoring	189
15.10	TSF physical protection (FPT_PHP)	190
15.10.1	Family Behaviour	190
15.10.2	Component levelling and description	190
15.10.3	Component management	190
15.10.4	Component audit	191
15.10.5	Application notes	191
15.10.6	FPT_PHP.1 Passive detection of physical attack	191
15.10.7	FPT_PHP.2 Notification of physical attack	192
15.10.8	FPT_PHP.3 Resistance to physical attack	193
15.11	Trusted recovery (FPT_RCV)	193
15.11.1	Family Behaviour	193
15.11.2	Component levelling and description	193

## ISO/IEC 15408-2:2026(en)

15.11.3	Component management .....	194
15.11.4	Component audit .....	194
15.11.5	Application notes .....	195
15.11.6	Evaluator notes .....	196
15.11.7	FPT_RCV.1 Manual recovery .....	196
15.11.8	FPT_RCV.2 Automated recovery .....	197
15.11.9	FPT_RCV.3 Automated recovery without undue loss .....	197
15.11.10	.....	
	FPT_RCV.4 Function recovery .....	198
15.12	Replay detection (FPT_RPL) .....	199
15.12.1	Family Behaviour .....	199
15.12.2	Component levelling and description .....	199
15.12.3	Component management .....	199
15.12.4	Component audit .....	199
15.12.5	Application notes .....	199
15.12.6	FPT_RPL.1 Replay detection .....	199
15.13	State synchrony protocol (FPT_SSP) .....	200
15.13.1	Family Behaviour .....	200
15.13.2	Component levelling and description .....	200
15.13.3	Component management .....	200
15.13.4	Component audit .....	200
15.13.5	Application notes .....	201
15.13.6	FPT_SSP.1 Simple trusted acknowledgement .....	201
15.13.7	FPT_SSP.2 Mutual trusted acknowledgement .....	201
15.14	Time stamps (FPT_STM) .....	202
15.14.1	Family Behaviour .....	202
15.14.2	Component levelling and description .....	202
15.14.3	Component management .....	202
15.14.4	Component audit .....	203
15.14.5	Application notes .....	203
15.14.6	FPT_STM.1 Reliable time stamps .....	203
15.14.7	FPT_STM.2 Time source .....	203
15.15	Inter-TSF TSF data consistency (FPT_TDC) .....	204
15.15.1	Family Behaviour .....	204
15.15.2	Component levelling and description .....	204
15.15.3	Component management .....	204
15.15.4	Component audit .....	204
15.15.5	Application notes .....	204
15.15.6	FPT_TDC.1 Inter-TSF basic TSF data consistency .....	205
15.16	Testing of external entities (FPT_TEE) .....	205
15.16.1	Family Behaviour .....	205
15.16.2	Component levelling and description .....	206
15.16.3	Component management .....	206
15.16.4	Component audit .....	206
15.16.5	Application notes .....	206
15.16.6	Evaluator notes .....	206
15.16.7	FPT_TEE.1 Testing of external entities .....	207
15.17	Internal TOE TSF data replication consistency (FPT_TRC) .....	208
15.17.1	Family Behaviour .....	208
15.17.2	Component levelling and description .....	208
15.17.3	Component management .....	208
15.17.4	Component audit .....	208
15.17.5	Application notes .....	208
15.17.6	FPT_TRC.1 Internal TSF consistency .....	209
15.18	TSF self-test (FPT_TST) .....	209
15.18.1	Family Behaviour .....	209
15.18.2	Component levelling and description .....	209
15.18.3	Component management .....	210
15.18.4	Component audit .....	210

	15.18.5 Application notes .....	210
	15.18.6 Evaluator notes .....	210
	15.18.7 FPT_TST.1 TSF self-testing .....	210
<b>16</b>	<b>Class FRU Resource utilization .....</b>	<b>211</b>
	16.1 Introduction .....	211
	16.2 Notes on class FRU .....	212
	16.3 Fault tolerance (FRU_FLT) .....	212
	16.3.1 Family Behaviour .....	212
	16.3.2 Component levelling and description .....	213
	16.3.3 Component management .....	213
	16.3.4 Component audit .....	213
	16.3.5 Application notes .....	213
	16.3.6 FRU_FLT.1 Degraded fault tolerance .....	214
	16.3.7 FRU_FLT.2 Limited fault tolerance .....	214
	16.4 Priority of service (FRU_PRS) .....	215
	16.4.1 Family Behaviour .....	215
	16.4.2 Component levelling and description .....	215
	16.4.3 Component management .....	215
	16.4.4 Component audit .....	215
	16.4.5 Application notes .....	215
	16.4.6 FRU_PRS.1 Limited priority of service .....	216
	16.4.7 FRU_PRS.2 Full priority of service .....	216
	16.5 Resource allocation (FRU_RSA) .....	217
	16.5.1 Family Behaviour .....	217
	16.5.2 Component levelling and description .....	217
	16.5.3 Component management .....	217
	16.5.4 Component audit .....	217
	16.5.5 Application notes .....	217
	16.5.6 FRU_RSA.1 Maximum quotas .....	218
	16.5.7 FRU_RSA.2 Minimum and maximum quotas .....	219
<b>17</b>	<b>Class FTA TOE access .....</b>	<b>219</b>
	17.1 Introduction .....	219
	17.2 Notes on class FTA .....	221
	17.3 Limitation on scope of selectable attributes (FTA_LSA) .....	221
	17.3.1 Family Behaviour .....	221
	17.3.2 Component levelling and description .....	221
	17.3.3 Component management .....	221
	17.3.4 Component audit .....	221
	17.3.5 Application notes .....	221
	17.3.6 FTA_LSA.1 Limitation on scope of selectable attributes .....	222
	17.4 Limitation on multiple concurrent sessions (FTA_MCS) .....	222
	17.4.1 Family Behaviour .....	222
	17.4.2 Component levelling and description .....	222
	17.4.3 Component management .....	223
	17.4.4 Component audit .....	223
	17.4.5 Application notes .....	223
	17.4.6 FTA_MCS.1 Basic limitation on multiple concurrent sessions .....	223
	17.4.7 FTA_MCS.2 Per user attribute limitation on multiple concurrent sessions .....	224
	17.5 Session locking and termination (FTA_SSL) .....	224
	17.5.1 Family Behaviour .....	224
	17.5.2 Component levelling and description .....	224
	17.5.3 Component management .....	225
	17.5.4 Component audit .....	226
	17.5.5 Application notes .....	226
	17.5.6 FTA_SSL.1 TSF-initiated session locking .....	226
	17.5.7 FTA_SSL.2 User-initiated locking .....	227
	17.5.8 FTA_SSL.3 TSF-initiated termination .....	228
	17.5.9 FTA_SSL.4 User-initiated termination .....	228

## ISO/IEC 15408-2:2026(en)

17.6	TOE access banners (FTA_TAB)	229
17.6.1	Family Behaviour	229
17.6.2	Component levelling and description	229
17.6.3	Component management	229
17.6.4	Component audit	229
17.6.5	Application notes	229
17.6.6	FTA_TAB.1 Default TOE access banners	229
17.7	TOE access history (FTA_TAH)	230
17.7.1	Family Behaviour	230
17.7.2	Component levelling and description	230
17.7.3	Component management	230
17.7.4	Component audit	230
17.7.5	Application notes	230
17.7.6	FTA_TAH.1 TOE access history	230
17.8	TOE session establishment (FTA_TSE)	231
17.8.1	Family Behaviour	231
17.8.2	Component levelling and description	231
17.8.3	Component management	231
17.8.4	Component audit	231
17.8.5	Application notes	232
17.8.6	FTA_TSE.1 TOE session establishment	232
<b>18</b>	<b>Class FTP Trusted path/channels</b>	<b>233</b>
18.1	Introduction	233
18.2	Notes on class FTP	234
18.3	Inter-TSF trusted channel (FTP_ITC)	234
18.3.1	Family Behaviour	234
18.3.2	Component levelling and description	234
18.3.3	Component management	235
18.3.4	Component audit	235
18.3.5	Application notes	235
18.3.6	FTP_ITC.1 Inter-TSF trusted channel	235
18.4	Trusted channel protocol (FTP_PRO)	236
18.4.1	Family Behaviour	236
18.4.2	Component levelling and description	236
18.4.3	Component management	236
18.4.4	Component audit	237
18.4.5	Application notes	237
18.4.6	FTP_PRO.1 Trusted channel protocol	238
18.4.7	FTP_PRO.2 Trusted channel establishment	239
18.4.8	FTP_PRO.3 Trusted channel data protection	240
18.5	Trusted path (FTP_TRP)	240
18.5.1	Family Behaviour	240
18.5.2	Component levelling and description	240
18.5.3	Component management	241
18.5.4	Component audit	241
18.5.5	Application notes	241
18.5.6	FTP_TRP.1 Trusted path	241
	<b>Bibliography</b>	<b>243</b>

## Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see [www.iso.org/directives](http://www.iso.org/directives) or [www.iec.ch/members\\_experts/refdocs](http://www.iec.ch/members_experts/refdocs)).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at [www.iso.org/patents](http://www.iso.org/patents) and <https://patents.iec.ch>. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see [www.iso.org/iso/foreword.html](http://www.iso.org/iso/foreword.html). In the IEC, see [www.iec.ch/understanding-standards](http://www.iec.ch/understanding-standards).

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*, in collaboration with the European Committee for Standardization (CEN) Technical Committee CEN/CLC/JTC 13, *Cybersecurity and data protection*, in accordance with the Agreement on technical cooperation between ISO and CEN (Vienna Agreement).

This fifth edition cancels and replaces the fourth edition (ISO/IEC 15408-2:2022), which has been technically revised.

The main changes are as follows:

- the document has been restructured;
- technical changes have been introduced:
  - the terminology has been reviewed and updated;
  - the dependency and hierarchy for each component have been reviewed and updated;
  - the new notes for operations have been introduced.

A list of all parts in the ISO/IEC 15408 series can be found on the ISO and IEC websites.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at [www.iso.org/members.html](http://www.iso.org/members.html) and [www.iec.ch/national-committees](http://www.iec.ch/national-committees).

## Introduction

Security functional components, as defined in this document, are the basis for the security functional requirements (SFRs) or components expressed in a Protection Profile (PP), PP-Module, functional package or a Security Target (ST). These requirements describe the desired security behaviour expected of a Target of Evaluation (TOE) and are intended to meet the security objectives as stated in a PP, PP-Module, functional package or an ST. These requirements describe security properties that users can detect by direct interaction (i.e. inputs, outputs) with the Information Technology (IT) or by the IT response to stimulus.

Security functional components allow for the expression of SFRs intended to counter threats in the assumed operating environment of the TOE and cover any identified organizational security policies.

The audience for this document includes consumers, developers and evaluators of secure IT products. ISO/IEC 15408-1 provides additional information on the target audience of the ISO/IEC 15408 series, and on the use of the ISO/IEC 15408 series by the groups that comprise the target audience. These groups use this document as follows:

- consumers, who use this document when selecting components to express functional requirements which satisfy the security objectives expressed in a PP, PP-Module, functional package or ST. ISO/IEC 15408-1 provides more detailed information on the relationship between security objectives and security requirements;
- developers, who respond to actual or perceived consumer security requirements in constructing a TOE and will find a standardized method to understand those requirements in this document. They also use the contents of this document as a basis for further defining the TOE security functionality and mechanisms that conform with those requirements;
- evaluators, who use the SFRs defined in this document in verifying that the TOE functional requirements expressed in the PP, PP-Module, functional package or ST satisfy the IT security objectives and that all dependencies are accounted for and shown to be satisfied. Evaluators use this document to assist in determining whether a given TOE satisfies stated requirements.

This document uses bold type to highlight hierarchical relationships between requirements. This convention calls for the use of bold type for all new requirements.

For security functional requirements, the use of italics denotes assignment and selection items.

Several governmental organizations have contributed to the development of this version of the Common Criteria for Information Technology Security Evaluations. As the joint holders of the copyright in the Common Criteria for Information Technology Security Evaluations (called CC), they hereby grant non-exclusive license to ISO/IEC to use CC in the continued development/maintenance of the ISO/IEC 15408 series of standards. However, these governmental organizations retain the right to use, copy, distribute, translate, or modify CC as they see fit. More information on these agencies can be found at <https://commoncriteriaportal.org/cc/copyright/index.cfm>.

# Information security, cybersecurity and privacy protection — Evaluation criteria for IT security —

## Part 2: Security functional components

### 1 Scope

This document specifies requirements for the required structure and content of security functional components for use during a security evaluation. It includes a catalogue of functional components that meet the common security functionality requirements of many IT products.

### 2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 15408-1:2026, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 1: Introduction and general model*

ISO/IEC 15408-3:2026, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 3: Security assurance components*

ISO/IEC 18045:2026, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Requirements and methodology for IT security evaluation*

## Bibliography

- [1] AIS 31, *Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren. Version 3, May 15, 2020*
- [2] ISO/IEC 9594-8, *Information technology — Open systems interconnection — Part 8: The Directory: Public-key and attribute certificate frameworks*
- [3] ISO/IEC 15408-4:2026, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 4: Framework for the specification of evaluation methods and activities*
- [4] ISO/IEC 15408-5:2026, *Information security — Evaluation criteria for IT security — Part 5: Pre-defined packages of security requirements*
- [5] ISO/IEC/TS 19249, *Information technology — Security techniques — Catalogue of architectural and design principles for secure products, systems and applications*
- [6] ISO/IEC/TS 19608, *Guidance for developing security and privacy functional requirements based on ISO/IEC 15408*
- [7] ISO/IEC 29100, *Information technology — Security techniques — Privacy framework*
- [8] ITU-T Recommendation X.509, *Information technology – Open systems interconnection – The directory: Public-key and attribute certificate frameworks.*
- [9] NIST SP 800-90A, *The National Institute of Standards and Technology (NIST). Special Publication 800-90A Recommendation for Random Number Generation Using Deterministic Random Bit Generators, June 2015*
- [10] NIST SP 800-90B, *The National Institute of Standards and Technology (NIST). Special Publication 800-90B Recommendation for the Entropy Sources Used for Random Bit Generation, January 2018*