

SLOVENSKI STANDARD

SIST EN ISO/IEC 15408-2:2026

01-oktober-2026

Nadomešča:

SIST EN ISO/IEC 15408-2:2024

Informacijska varnost, kibernetika varnost in varstvo zasebnosti - Merila za vrednotenje varnosti IT - 2. del: Funkcionalne varnostne komponente (ISO/IEC 15408-2:2026)

Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Part 2: Security functional components (ISO/IEC 15408-2:2026)

Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre - Evaluationskriterien für IT-Sicherheit - Teil 2: Sicherheitsfunktionskomponenten (ISO/IEC 15408-2:2026)

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 (ISO/IEC 15408-2:2026)

Ta slovenski standard je istoveten z: EN ISO/IEC 15408-2:2026

ICS:

35.030	Informacijska varnost	IT Security
--------	-----------------------	-------------

SIST EN ISO/IEC 15408-2:2026	en,fr,de
-------------------------------------	-----------------

Sample Document

get full document from standards.iteh.ai

EUROPEAN STANDARD

EN ISO/IEC 15408-2

NORME EUROPÉENNE

EUROPÄISCHE NORM

May 2026

ICS 35.030

Supersedes EN ISO/IEC 15408-2:2023

English version

Information security, cybersecurity and privacy protection
- Evaluation criteria for IT security - Part 2: Security
functional components (ISO/IEC 15408-2:2026)

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 (ISO/IEC 15408-
2:2026)

Informationssicherheit, Cybersicherheit und Schutz
der Privatsphäre - Evaluationskriterien für IT-
Sicherheit - Teil 2: Sicherheitsfunktionskomponenten
(ISO/IEC 15408-2:2026)

This European Standard was approved by CEN on 1 May 2026.

CEN and CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN and CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN and CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN and CENELEC members are the national standards bodies and national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and United Kingdom.



CEN-CENELEC Management Centre:
Rue de la Science 23, B-1040 Brussels

EN ISO/IEC 15408-2:2026 (E)

Contents	Page
European foreword.....	3

Sample Document

get full document from standards.iteh.ai

European foreword

This document (EN ISO/IEC 15408-2:2026) has been prepared by Technical Committee ISO/IEC JTC 1 "Information technology" in collaboration with Technical Committee CEN-CENELEC/ JTC 13 "Cybersecurity and Data Protection" the secretariat of which is held by DIN.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by November 2026, and conflicting national standards shall be withdrawn at the latest by November 2026.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN-CENELEC shall not be held responsible for identifying any or all such patent rights.

This document supersedes EN ISO/IEC 15408-2:2023.

Any feedback and questions on this document should be directed to the users' national standards body/national committee. A complete listing of these bodies can be found on the CEN and CENELEC websites.

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and the United Kingdom.

Endorsement notice

The text of ISO/IEC 15408-2:2026 has been approved by CEN-CENELEC as EN ISO/IEC 15408-2:2026 without any modification.

Sample Document

get full document from standards.iteh.ai



**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**

ISO/IEC 15408-2:2026(en)

Sample Document

get full document from standards.iteh.ai

**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
Website: www.iso.org

Published in Switzerland

© ISO/IEC 2026 – All rights reserved

ISO/IEC 15408-2:2026(en)

Contents

Page

Foreword	xv
Introduction	xvi
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Abbreviated terms	3
5 Overview	4
5.1 General	4
5.2 Organization of this document	4
6 Functional requirements paradigm	5
7 Security functional components	8
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
8 Class FAU Security audit	15
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
9	Class FCO Communication	38
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
10	Class FCS Cryptographic support	46
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
11	Class FDP User data protection	66
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

ISO/IEC 15408-2:2026(en)

12	Class FIA Identification and authentication	117
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

ISO/IEC 15408-2:2026(en)

	12.9.6 FIA_USB.1 User-subject binding.....	135
13	Class FMT Security management	136
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