

INTERNATIONAL STANDARD

ISO/IEC
15408-3

Second edition
2005-10-01

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

Part 3: Security assurance requirements

iTeh STANDARD PREVIEW
*Technologies de l'information — Techniques de sécurité — Critères
d'évaluation pour la sécurité TI —
Partie 3: Exigences d'assurance de sécurité*

[ISO/IEC 15408-3:2005](#)
[https://standards.iteh.ai/catalog/standards/sist/271f4084-efa5-4245-bace-
b5f8851addee/iso-iec-15408-3-2005](https://standards.iteh.ai/catalog/standards/sist/271f4084-efa5-4245-bace-b5f8851addee/iso-iec-15408-3-2005)

Reference number
ISO/IEC 15408-3:2005(E)



© ISO/IEC 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 15408-3:2005](#)

<https://standards.iteh.ai/catalog/standards/sist/271f4084-efa5-4245-bace-b5f8851addee/iso-iec-15408-3-2005>

© 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	ix
Introduction.....	xi
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 ISO/IEC 15408 assurance paradigm	2
5.1 ISO/IEC 15408 philosophy	2
5.2 Assurance approach	2
5.2.1 Significance of vulnerabilities.....	2
5.2.2 Cause of vulnerabilities	3
5.2.3 ISO/IEC 15408 assurance	3
5.2.4 Assurance through evaluation.....	3
5.3 ISO/IEC 15408 evaluation assurance scale	3
6 Security assurance requirements.....	4
6.1 Structures.....	4
6.1.1 Class structure	4
6.1.2 Assurance family structure	5
6.1.3 Assurance component structure	6
6.1.4 Assurance elements.....	8
6.1.5 EAL structure.....	8
6.2 Component taxonomy.....	10
6.3 Protection Profile and Security Target evaluation criteria class structure	11
6.4 Usage of terms in this part of ISO/IEC 15408	11
6.5 Assurance categorisation	13
6.6 Assurance class and family overview.....	13
6.6.1 Class ACM:Configuration management.....	13
6.6.2 Class ADO:Delivery and operation.....	14
6.6.3 Class ADV:Development.....	14
6.6.4 Class AGD:Guidance documents	15
6.6.5 Class ALC:Life cycle support	15
6.6.6 Class APE:Protection Profile evaluation	16
6.6.7 Class ASE:Security Target evaluation	16
6.6.8 Class ATE:Tests	16
6.6.9 Class AVA:Vulnerability assessment.....	17
7 Protection Profile and Security Target evaluation criteria.....	17
7.1 Overview.....	17
7.2 Protection Profile criteria overview	18
7.2.1 Protection Profile evaluation.....	18
7.2.2 Relation to the Security Target evaluation criteria	18
7.2.3 Evaluator tasks	18
7.3 Security Target criteria overview	19
7.3.1 Security Target evaluation	19
7.3.2 Relation to the other evaluation criteria in this part of ISO/IEC 15408	19
7.3.3 Evaluator tasks	19
8 Class APE: Protection Profile evaluation	20
8.1 TOE description (APE_DES)	20

8.1.1	Objectives	20
8.1.2	APE_DES.1 Protection Profile, TOE description, Evaluation requirements	21
8.2	Security environment (APE_ENV)	21
8.2.1	Objectives	21
8.2.2	APE_ENV.1 Protection Profile, Security environment, Evaluation requirements	21
8.3	PP introduction (APE_INT)	22
8.3.1	Objectives	22
8.3.2	APE_INT.1 Protection Profile, PP introduction, Evaluation requirements	22
8.4	Security objectives (APE_OBJ)	23
8.4.1	Objectives	23
8.4.2	APE_OBJ.1 Protection Profile, Security objectives, Evaluation requirements	23
8.5	IT security requirements (APE_REQ)	24
8.5.1	Objectives	24
8.5.2	Application notes	24
8.5.3	APE_REQ.1 Protection Profile, IT security requirements, Evaluation requirements	25
8.6	Explicitly stated IT security requirements (APE_SRE)	26
8.6.1	Objectives	26
8.6.2	Application notes	26
8.6.3	APE_SRE.1 Protection Profile, Explicitly stated IT security requirements, Evaluation requirements	27
9	Class ASE: Security Target evaluation	28
9.1	TOE description (ASE_Des)	29
9.1.1	Objectives	29
9.1.2	ASE_Des.1 Security Target, TOE description, Evaluation requirements	29
9.2	Security environment (ASE_ENV)	29
9.2.1	Objectives	29
9.2.2	ASE_ENV.1 Security Target, Security environment, Evaluation requirements	30
9.3	ST introduction (ASE_INT)	30
9.3.1	Objectives	30
9.3.2	ASE_INT.1 Security Target, ST introduction, Evaluation requirements	30
9.4	Security objectives (ASE_OBJ)	31
9.4.1	Objectives	31
9.4.2	ASE_OBJ.1 Security Target, Security objectives, Evaluation requirements	31
9.5	PP claims (ASE_PPC)	32
9.5.1	Objectives	32
9.5.2	Application notes	32
9.5.3	ASE_PPC.1 Security Target, PP claims, Evaluation requirements	33
9.6	IT security requirements (ASE_REQ)	33
9.6.1	Objectives	33
9.6.2	Application notes	34
9.6.3	ASE_REQ.1 Security Target, IT security requirements, Evaluation requirements	34
9.7	Explicitly stated IT security requirements (ASE_SRE)	35
9.7.1	Objectives	35
9.7.2	Application notes	36
9.7.3	ASE_SRE.1 Security Target, Explicitly stated IT security requirements, Evaluation requirements	36
9.8	TOE summary specification (ASE_TSS)	37
9.8.1	Objectives	37
9.8.2	Application notes	37
9.8.3	ASE_TSS.1 Security Target, TOE summary specification, Evaluation requirements	38
10	Evaluation assurance levels	39
10.1	Evaluation assurance level (EAL) overview	39
10.2	Evaluation assurance level details	40
10.3	Evaluation assurance level 1 (EAL1) - functionally tested	40
10.3.1	Objectives	40
10.3.2	Assurance components	41
10.4	Evaluation assurance level 2 (EAL2) - structurally tested	41
10.4.1	Objectives	41
10.4.2	Assurance components	41

10.5	Evaluation assurance level 3 (EAL3) - methodically tested and checked.....	42
10.5.1	Objectives	42
10.5.2	Assurance components.....	42
10.6	Evaluation assurance level 4 (EAL4) - methodically designed, tested, and reviewed.....	43
10.6.1	Objectives	43
10.6.2	Assurance components.....	43
10.7	Evaluation assurance level 5 (EAL5) - semiformally designed and tested	44
10.7.1	Objectives	44
10.7.2	Assurance components.....	44
10.8	Evaluation assurance level 6 (EAL6) - semiformally verified design and tested.....	45
10.8.1	Objectives	45
10.8.2	Assurance components.....	45
10.9	Evaluation assurance level 7 (EAL7) - formally verified design and tested.....	46
10.9.1	Objectives	46
10.9.2	Assurance components.....	46
11	Assurance classes, families, and components.....	47
12	Class ACM: Configuration management.....	47
12.1	CM automation (ACM_AUT).....	48
12.1.1	Objectives	48
12.1.2	Component levelling	48
12.1.3	Application notes	48
12.1.4	ACM_AUT.1 Partial CM automation	48
12.1.5	ACM_AUT.2 Complete CM automation	49
12.2	CM capabilities (ACM_CAP)	50
12.2.1	Objectives	50
12.2.2	Component levelling	51
12.2.3	Application notes	51
12.2.4	ACM_CAP.1 Version numbers	51
12.2.5	ACM_CAP.2 Configuration items	52
12.2.6	ACM_CAP.3 Authorisation controls	53
12.2.7	ACM_CAP.4 Generation support and acceptance procedures	54
12.2.8	ACM_CAP.5 Advanced support	56
12.3	CM scope (ACM_SCP).....	59
12.3.1	Objectives	59
12.3.2	Component levelling	59
12.3.3	Application notes	59
12.3.4	ACM_SCP.1 TOE CM coverage	59
12.3.5	ACM_SCP.2 Problem tracking CM coverage	60
12.3.6	ACM_SCP.3 Development tools CM coverage	60
13	Class ADO: Delivery and operation.....	61
13.1	Delivery (ADO_DEL).....	61
13.1.1	Objectives	61
13.1.2	Component levelling	62
13.1.3	Application notes	62
13.1.4	ADO_DEL.1 Delivery procedures.....	62
13.1.5	ADO_DEL.2 Detection of modification	62
13.1.6	ADO_DEL.3 Prevention of modification	63
13.2	Installation, generation and start-up (ADO_IGS)	64
13.2.1	Objectives	64
13.2.2	Component levelling	64
13.2.3	Application notes	64
13.2.4	ADO_IGS.1 Installation, generation, and start-up procedures	64
13.2.5	ADO_IGS.2 Generation log	65
14	Class ADV: Development.....	66
14.1	Functional specification (ADV_FSP)	70
14.1.1	Objectives	70
14.1.2	Component levelling	70
14.1.3	Application notes	70

14.1.4	ADV_FSP.1 Informal functional specification.....	71
14.1.5	ADV_FSP.2 Fully defined external interfaces	71
14.1.6	ADV_FSP.3 Semiformal functional specification	72
14.1.7	ADV_FSP.4 Formal functional specification.....	73
14.2	High-level design (ADV_HLD).....	74
14.2.1	Objectives.....	74
14.2.2	Component levelling	74
14.2.3	Application notes.....	74
14.2.4	ADV_HLD.1 Descriptive high-level design	75
14.2.5	ADV_HLD.2 Security enforcing high-level design.....	76
14.2.6	ADV_HLD.3 Semiformal high-level design.....	77
14.2.7	ADV_HLD.4 Semiformal high-level explanation	78
14.2.8	ADV_HLD.5 Formal high-level design	79
14.3	Implementation representation (ADV_IMP).....	81
14.3.1	Objectives.....	81
14.3.2	Component levelling	81
14.3.3	Application notes.....	81
14.3.4	ADV_IMP.1 Subset of the implementation of the TSF.....	81
14.3.5	ADV_IMP.2 Implementation of the TSF	82
14.3.6	ADV_IMP.3 Structured implementation of the TSF	83
14.4	TSF internals (ADV_INT)	84
14.4.1	Objectives.....	84
14.4.2	Component levelling	84
14.4.3	Application notes.....	84
14.4.4	ADV_INT.1 Modularity	85
14.4.5	ADV_INT.2 Reduction of complexity.....	86
14.4.6	ADV_INT.3 Minimisation of complexity	87
14.5	Low-level design (ADV_LLD).....	89
14.5.1	Objectives.....	89
14.5.2	Component levelling	89
14.5.3	Application notes.....	ISO/IEC 15408-3:2005
14.5.4	ADV_LLD.1 Descriptive low-level design.....	89
14.5.5	ADV_LLD.2 Semiformal low-level design.....	91
14.5.6	ADV_LLD.3 Formal low-level design	92
14.6	Representation correspondence (ADV_RCR).....	93
14.6.1	Objectives.....	93
14.6.2	Component levelling	93
14.6.3	Application notes.....	93
14.6.4	ADV_RCR.1 Informal correspondence demonstration	94
14.6.5	ADV_RCR.2 Semiformal correspondence demonstration	94
14.6.6	ADV_RCR.3 Formal correspondence demonstration	95
14.7	Security policy modeling (ADV_SPM)	96
14.7.1	Objectives.....	96
14.7.2	Component levelling	96
14.7.3	Application notes.....	96
14.7.4	ADV_SPM.1 Informal TOE security policy model.....	96
14.7.5	ADV_SPM.2 Semiformal TOE security policy model	97
14.7.6	ADV_SPM.3 Formal TOE security policy model	98
15	Class AGD: Guidance documents	99
15.1	Administrator guidance (AGD_ADM).....	99
15.1.1	Objectives.....	99
15.1.2	Component levelling	99
15.1.3	Application notes.....	99
15.1.4	AGD_ADM.1 Administrator guidance	100
15.2	User guidance (AGD_USR)	101
15.2.1	Objectives.....	101
15.2.2	Component levelling	101
15.2.3	Application notes.....	101
15.2.4	AGD_USR.1 User guidance	101

16	Class ALC: Life cycle support	102
16.1	Development security (ALC_DVS).....	102
16.1.1	Objectives	102
16.1.2	Component levelling	102
16.1.3	Application notes	103
16.1.4	ALC_DVS.1 Identification of security measures	103
16.1.5	ALC_DVS.2 Sufficiency of security measures	103
16.2	Flaw remediation (ALC_FLR)	104
16.2.1	Objectives	104
16.2.2	Component levelling	104
16.2.3	Application notes	104
16.2.4	ALC_FLR.1 Basic flaw remediation	105
16.2.5	ALC_FLR.2 Flaw reporting procedures.....	105
16.2.6	ALC_FLR.3 Systematic flaw remediation.....	107
16.3	Life cycle definition (ALC_LCD).....	108
16.3.1	Objectives	108
16.3.2	Component levelling	109
16.3.3	Application notes	109
16.3.4	ALC_LCD.1 Developer defined life-cycle model	109
16.3.5	ALC_LCD.2 Standardised life-cycle model.....	110
16.3.6	ALC_LCD.3 Measurable life-cycle model.....	111
16.4	Tools and techniques (ALC_TAT).....	112
16.4.1	Objectives	112
16.4.2	Component levelling	112
16.4.3	Application notes	112
16.4.4	ALC_TAT.1 Well-defined development tools	112
16.4.5	ALC_TAT.2 Compliance with implementation standards	113
16.4.6	ALC_TAT.3 Compliance with implementation standards - all parts	114
17	Class ATE: Tests	114
17.1	Coverage (ATE_COV)..... ISO/IEC 15408-3:2005	115
17.1.1	Objectives	115
17.1.2	Component levelling	115
17.1.3	ATE_COV.1 Evidence of coverage	115
17.1.4	ATE_COV.2 Analysis of coverage	116
17.1.5	ATE_COV.3 Rigorous analysis of coverage	117
17.2	Depth (ATE_DPT).....	118
17.2.1	Objectives	118
17.2.2	Component levelling	118
17.2.3	Application notes	118
17.2.4	ATE_DPT.1 Testing: high-level design.....	118
17.2.5	ATE_DPT.2 Testing: low-level design	119
17.2.6	ATE_DPT.3 Testing: implementation representation	120
17.3	Functional tests (ATE_FUN).....	121
17.3.1	Objectives	121
17.3.2	Component levelling	121
17.3.3	Application notes	121
17.3.4	ATE_FUN.1 Functional testing	122
17.3.5	ATE_FUN.2 Ordered functional testing.....	122
17.4	Independent testing (ATE_IND)	124
17.4.1	Objectives	124
17.4.2	Component levelling	124
17.4.3	Application notes	124
17.4.4	ATE_IND.1 Independent testing - conformance	125
17.4.5	ATE_IND.2 Independent testing - sample	125
17.4.6	ATE_IND.3 Independent testing - complete.....	126
18	Class AVA: Vulnerability assessment.....	127
18.1	Covert channel analysis (AVA_CCA)	128
18.1.1	Objectives	128
18.1.2	Component levelling	128

18.1.3 Application notes.....	128
18.1.4 AVA_CCA.1 Covert channel analysis	128
18.1.5 AVA_CCA.2 Systematic covert channel analysis.....	130
18.1.6 AVA_CCA.3 Exhaustive covert channel analysis.....	130
18.2 Misuse (AVA_MSU).....	132
18.2.1 Objectives.....	132
18.2.2 Component levelling	132
18.2.3 Application notes.....	132
18.2.4 AVA_MSU.1 Examination of guidance	133
18.2.5 AVA_MSU.2 Validation of analysis	134
18.2.6 AVA_MSU.3 Analysis and testing for insecure states	135
18.3 Strength of TOE security functions (AVA_SOF).....	137
18.3.1 Objectives.....	137
18.3.2 Component levelling	137
18.3.3 Application notes.....	137
18.3.4 AVA_SOF.1 Strength of TOE security function evaluation	137
18.4 Vulnerability analysis (AVA_VLA).....	138
18.4.1 Objectives.....	138
18.4.2 Component levelling	138
18.4.3 Application notes.....	138
18.4.4 AVA_VLA.1 Developer vulnerability analysis	139
18.4.5 AVA_VLA.2 Independent vulnerability analysis	140
18.4.6 AVA_VLA.3 Moderately resistant.....	141
18.4.7 AVA_VLA.4 Highly resistant.....	142
Annex A (informative) Cross reference of assurance component dependencies.....	145
Annex B (informative) Cross reference of EALs and assurance components	149

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[ISO/IEC 15408-3:2005](#)

<https://standards.iteh.ai/catalog/standards/sist/271f4084-efa5-4245-bace-b5f8851addee/iso-iec-15408-3-2005>

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. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

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

ISO/IEC 15408-3 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT security techniques*. The identical text of ISO/IEC 15408 is published by the Common Criteria Project Sponsoring Organisations as Common Criteria for Information/Technology Security Evaluation.

THE STANDARD PREVIEW

This second edition cancels and replaces the first edition (ISO/IEC 15408-3:1999), which has been technically revised.

ISO/IEC 15408 consists of the following parts, under the general title *Information technology — Security techniques — Evaluation criteria for IT security*:
<https://standards.iec.ch/catalog/standards/sist/2714084-efab-4245-base-b518831addee/iso-iec-15408-3-2005>

- *Part 1: Introduction and general model*
- *Part 2: Security functional requirements*
- *Part 3: Security assurance requirements*

Legal notice

The governmental organizations listed below 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, version 2.3 Parts 1 through 3 (called CC 2.3), they hereby grant non-exclusive license to ISO/IEC to use CC 2.3 in the continued development/maintenance of the ISO/IEC 15408 international standard. However, these governmental organizations retain the right to use, copy, distribute, translate or modify CC 2.3 as they see fit.

Australia/New Zealand: The Defence Signals Directorate and the Government Communications Security Bureau respectively;

Canada: Communications Security Establishment;

France:	Direction Centrale de la Sécurité des Systèmes d'Information;
Germany:	Bundesamt für Sicherheit in der Informationstechnik;
Japan:	Information Technology Promotion Agency;
Netherlands:	Netherlands National Communications Security Agency;
Spain:	Ministerio de Administraciones Públicas and Centro Criptológico Nacional;
United Kingdom:	Communications-Electronic Security Group;
United States:	The National Security Agency and the National Institute of Standards and Technology.

iTeh STANDARD PREVIEW (standards.iteh.ai)

[ISO/IEC 15408-3:2005](#)

<https://standards.iteh.ai/catalog/standards/sist/271f4084-efa5-4245-bace-b5f8851addee/iso-iec-15408-3-2005>

Introduction

Security assurance components, as defined in this part of ISO/IEC 15408, are the basis for the security assurance requirements expressed in a Protection Profile (PP) or a Security Target (ST).

These requirements establish a standard way of expressing the assurance requirements for TOEs. This part of ISO/IEC 15408 catalogues the set of assurance components, families and classes. This part of ISO/IEC 15408 also defines evaluation criteria for PPs and STs and presents evaluation assurance levels that define the predefined ISO/IEC 15408 scale for rating assurance for TOEs, which is called the Evaluation Assurance Levels (EALs).

The audience for this part of ISO/IEC 15408 includes consumers, developers, and evaluators of secure IT systems and products. ISO/IEC 15408-1 Clause 5 provides additional information on the target audience of ISO/IEC 15408, and on the use of ISO/IEC 15408 by the groups that comprise the target audience. These groups may use this part of ISO/IEC 15408 as follows:

- a) Consumers, who use this part of ISO/IEC 15408 when selecting components to express assurance requirements to satisfy the security objectives expressed in a PP or ST, determining required levels of security assurance of the TOE. ISO/IEC 15408-1 Subclause 5.3 provides more detailed information on the relationship between security objectives and security requirements.
- b) Developers, who respond to actual or perceived consumer security requirements in constructing a TOE, reference this part of ISO/IEC 15408 when interpreting statements of assurance requirements and determining assurance approaches of TOEs.
- c) Evaluators, who use the assurance requirements defined in this part of ISO/IEC 15408 as mandatory statement of evaluation criteria when determining the assurance of TOEs and when evaluating PPs and STs.

ISO/IEC 15408-3:2005
<https://standards.iteh.ai/catalog/standards/sist/271f4084-efaf-4245-bace-b5f8851addee/iso-iec-15408-3-2005>

iTeh STANDARD PREVIEW (standards.iteh.ai)

[ISO/IEC 15408-3:2005](#)

<https://standards.iteh.ai/catalog/standards/sist/271f4084-efa5-4245-bace-b5f8851addee/iso-iec-15408-3-2005>

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

Part 3: Security assurance requirements

1 Scope

This part of ISO/IEC 15408 defines the assurance requirements of ISO/IEC 15408. It includes the evaluation assurance levels (EALs) that define a scale for measuring assurance, the individual assurance components from which the assurance levels are composed, and the criteria for evaluation of PPs and STs.

2 Normative references

The following referenced documents are indispensable for the application 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, *Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model*

3 Terms, definitions, symbols and abbreviated terms

For the purposes of this document, the terms, definitions, symbols and abbreviated terms given in ISO/IEC 15408-1 apply.

<https://standards.iteh.ai/catalog/standards/sist/271f4084-efab-4245-bace-b5f8851addee/iso-iec-15408-3-2005>

4 Overview

4.1 Organisation of this part of ISO/IEC 15408

Clause 5 describes the paradigm used in the security assurance requirements of this part of ISO/IEC 15408.

Clause 6 describes the presentation structure of the assurance classes, families, components, and evaluation assurance levels along with their relationships. It also characterises the assurance classes and families found in clauses 12 through 18.

Clauses 7, 8 and 9 provide a brief introduction to the evaluation criteria for PPs and STs, followed by detailed explanations of the families and components that are used for those evaluations.

Clause 10 provides detailed definitions of the EALs.

Clause 11 provides a brief introduction to the assurance classes and is followed by clauses 12 through 18 that provide detailed definitions of those classes.

Annex A provides a summary of the dependencies between the assurance components.

Annex B provides a cross reference between the EALs and the assurance components.

5 ISO/IEC 15408 assurance paradigm

The purpose of this clause is to document the philosophy that underpins ISO/IEC 15408 approach to assurance. An understanding of this clause will permit the reader to understand the rationale behind this part of ISO/IEC 15408 assurance requirements.

5.1 ISO/IEC 15408 philosophy

ISO/IEC 15408 philosophy is that the threats to security and organisational security policy commitments should be clearly articulated and the proposed security measures be demonstrably sufficient for their intended purpose.

Furthermore, measures should be adopted that reduce the likelihood of vulnerabilities, the ability to exercise (i.e. intentionally exploit or unintentionally trigger) a vulnerability, and the extent of the damage that could occur from a vulnerability being exercised. Additionally, measures should be adopted that facilitate the subsequent identification of vulnerabilities and the elimination, mitigation, and/or notification that a vulnerability has been exploited or triggered.

5.2 Assurance approach

ISO/IEC 15408 philosophy is to provide assurance based upon an evaluation (active investigation) of the IT product or system that is to be trusted. Evaluation has been the traditional means of providing assurance and is the basis for prior evaluation criteria documents. In aligning the existing approaches, ISO/IEC 15408 adopts the same philosophy. ISO/IEC 15408 proposes measuring the validity of the documentation and of the resulting IT product or system by expert evaluators with increasing emphasis on scope, depth, and rigour.

ISO/IEC 15408 does not exclude, nor does it comment upon, the relative merits of other means of gaining assurance. Research continues with respect to alternative ways of gaining assurance. As mature alternative approaches emerge from these research activities, they will be considered for inclusion in ISO/IEC 15408, which is so structured as to allow their future introduction.
The STANDARD PREVIEW
(standards.iteh.ai)

<https://standards.iteh.ai/catalog/standards/sist/271f4084-efa5-4245-bace->

5.2.1 Significance of vulnerabilities b5f8851addee/iso-iec-15408-3-2005

It is assumed that there are threat agents that will actively seek to exploit opportunities to violate security policies both for illicit gains and for well-intentioned, but nonetheless insecure actions. Threat agents may also accidentally trigger security vulnerabilities, causing harm to the organisation. Due to the need to process sensitive information and the lack of availability of sufficiently trusted products or systems, there is significant risk due to failures of IT. It is, therefore, likely that IT security breaches could lead to significant loss.

IT security breaches arise through the intentional exploitation or the unintentional triggering of vulnerabilities in the application of IT within business concerns.

Steps should be taken to prevent vulnerabilities arising in IT products and systems. To the extent feasible, vulnerabilities should be:

- a) eliminated — that is, active steps should be taken to expose, and remove or neutralise, all exercisable vulnerabilities;
- b) minimised — that is, active steps should be taken to reduce, to an acceptable residual level, the potential impact of any exercise of a vulnerability;
- c) monitored — that is, active steps should be taken to ensure that any attempt to exercise a residual vulnerability will be detected so that steps can be taken to limit the damage.

5.2.2 Cause of vulnerabilities

Vulnerabilities can arise through failures in:

- a) requirements — that is, an IT product or system may possess all the functions and features required of it and still contain vulnerabilities that render it unsuitable or ineffective with respect to security;
- b) construction — that is, an IT product or system does not meet its specifications and/or vulnerabilities have been introduced as a result of poor constructional standards or incorrect design choices;
- c) operation — that is, an IT product or system has been constructed correctly to a correct specification but vulnerabilities have been introduced as a result of inadequate controls upon the operation.

5.2.3 ISO/IEC 15408 assurance

Assurance is grounds for confidence that an IT product or system meets its security objectives. Assurance can be derived from reference to sources such as unsubstantiated assertions, prior relevant experience, or specific experience. However, ISO/IEC 15408 provides assurance through active investigation. Active investigation is an evaluation of the IT product or system in order to determine its security properties.

5.2.4 Assurance through evaluation

Evaluation has been the traditional means of gaining assurance, and is the basis of ISO/IEC 15408 approach. Evaluation techniques can include, but are not limited to:

- a) analysis and checking of process(es) and procedure(s);
iTech STANDARD PREVIEW
(standards.iteh.ai)
- b) checking that process(es) and procedure(s) are being applied;
- c) analysis of the correspondence between TOE design representations;
ISO/IEC 15408-3:2005
<https://standards.iteh.ai/catalog/standards/sist/271f4084-ef45-4245-bace-031883#addcisoiec154083-2005>
- d) analysis of the TOE design representation against the requirements;
- e) verification of proofs;
- f) analysis of guidance documents;
- g) analysis of functional tests developed and the results provided;
- h) independent functional testing;
- i) analysis for vulnerabilities (including flaw hypothesis);
- j) penetration testing.

5.3 ISO/IEC 15408 evaluation assurance scale

ISO/IEC 15408 philosophy asserts that greater assurance results from the application of greater evaluation effort, and that the goal is to apply the minimum effort required to provide the necessary level of assurance. The increasing level of effort is based upon:

- a) scope — that is, the effort is greater because a larger portion of the IT product or system is included;
- b) depth — that is, the effort is greater because it is deployed to a finer level of design and implementation detail;
- c) rigour — that is, the effort is greater because it is applied in a more structured, formal manner.