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

Part 3: Security assurance components
National foreword

This British Standard is the UK implementation of ISO/IEC 15408-3:2022. It supersedes BS ISO/IEC 15408-3:2008, which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee IST/33/3, Security Evaluation, Testing and Specification.

A list of organizations represented on this committee can be obtained on request to its committee manager.

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient’s own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

© The British Standards Institution 2022
Published by BSI Standards Limited 2022

ISBN 978 0 580 99018 2

ICS 35.030

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 October 2022.

Amendments/corrigenda issued since publication

<table>
<thead>
<tr>
<th>Date</th>
<th>Text affected</th>
</tr>
</thead>
</table>
Information security, cybersecurity and privacy protection — Evaluation criteria for IT security —

Part 3:
Security assurance components
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Foreword</td>
<td>x</td>
</tr>
<tr>
<td>Introduction</td>
<td>xii</td>
</tr>
<tr>
<td>1 Scope</td>
<td>xii</td>
</tr>
<tr>
<td>2 Normative references</td>
<td>1</td>
</tr>
<tr>
<td>3 Terms and definitions</td>
<td>1</td>
</tr>
<tr>
<td>4 Overview</td>
<td>5</td>
</tr>
<tr>
<td>5 Assurance paradigm</td>
<td>6</td>
</tr>
<tr>
<td>5.1 General</td>
<td>6</td>
</tr>
<tr>
<td>5.2 ISO/IEC 15408 series approach</td>
<td>6</td>
</tr>
<tr>
<td>5.3 Assurance approach</td>
<td>6</td>
</tr>
<tr>
<td>5.3.1 General</td>
<td>6</td>
</tr>
<tr>
<td>5.3.2 Significance of vulnerabilities</td>
<td>6</td>
</tr>
<tr>
<td>5.3.3 Cause of vulnerabilities</td>
<td>7</td>
</tr>
<tr>
<td>5.3.4 ISO/IEC 15408 series assurance</td>
<td>7</td>
</tr>
<tr>
<td>5.3.5 Assurance through evaluation</td>
<td>7</td>
</tr>
<tr>
<td>5.4 ISO/IEC 15408 series evaluation assurance scale</td>
<td>8</td>
</tr>
<tr>
<td>6 Security assurance components</td>
<td>8</td>
</tr>
<tr>
<td>6.1 General</td>
<td>8</td>
</tr>
<tr>
<td>6.2 Assurance class structure</td>
<td>8</td>
</tr>
<tr>
<td>6.2.1 General</td>
<td>8</td>
</tr>
<tr>
<td>6.2.2 Class name</td>
<td>8</td>
</tr>
<tr>
<td>6.2.3 Class introduction</td>
<td>8</td>
</tr>
<tr>
<td>6.2.4 Assurance families</td>
<td>9</td>
</tr>
<tr>
<td>6.3 Assurance family structure</td>
<td>9</td>
</tr>
<tr>
<td>6.3.1 Family name</td>
<td>9</td>
</tr>
<tr>
<td>6.3.2 Objectives</td>
<td>9</td>
</tr>
<tr>
<td>6.3.3 Component levelling</td>
<td>10</td>
</tr>
<tr>
<td>6.3.4 Application notes</td>
<td>10</td>
</tr>
<tr>
<td>6.3.5 Assurance components</td>
<td>10</td>
</tr>
<tr>
<td>6.4 Assurance component structure</td>
<td>10</td>
</tr>
<tr>
<td>6.4.1 General</td>
<td>10</td>
</tr>
<tr>
<td>6.4.2 Component identification</td>
<td>11</td>
</tr>
<tr>
<td>6.4.3 Objectives</td>
<td>11</td>
</tr>
<tr>
<td>6.4.4 Application notes</td>
<td>11</td>
</tr>
<tr>
<td>6.4.5 Dependencies</td>
<td>11</td>
</tr>
<tr>
<td>6.4.6 Assurance elements</td>
<td>11</td>
</tr>
<tr>
<td>6.5 Assurance elements</td>
<td>12</td>
</tr>
<tr>
<td>6.6 Component taxonomy</td>
<td>12</td>
</tr>
<tr>
<td>7 Class APE: Protection Profile (PP) evaluation</td>
<td>12</td>
</tr>
<tr>
<td>7.1 General</td>
<td>12</td>
</tr>
<tr>
<td>7.2 PP introduction (APE_INT)</td>
<td>13</td>
</tr>
<tr>
<td>7.2.1 Objectives</td>
<td>13</td>
</tr>
<tr>
<td>7.2.2 APE_INT1 PP introduction</td>
<td>13</td>
</tr>
<tr>
<td>7.3 Conformance claims (APE_CCL)</td>
<td>14</td>
</tr>
<tr>
<td>7.3.1 Objectives</td>
<td>14</td>
</tr>
<tr>
<td>7.3.2 APE_CCL1 Conformance claims</td>
<td>14</td>
</tr>
<tr>
<td>7.4 Security problem definition (APE_SPD)</td>
<td>16</td>
</tr>
<tr>
<td>7.4.1 Objectives</td>
<td>16</td>
</tr>
<tr>
<td>7.4.2 APE_SPD1 Security problem definition</td>
<td>16</td>
</tr>
<tr>
<td>7.5 Security objectives (APE_OBJ)</td>
<td>16</td>
</tr>
<tr>
<td>7.5.1 Objectives</td>
<td>16</td>
</tr>
<tr>
<td>7.5.2 Component levelling</td>
<td>17</td>
</tr>
</tbody>
</table>
7.5.3 APE_OBJ.1 Security objectives for the operational environment ........................................ 17
7.5.4 APE_OBJ.2 Security objectives .......................................................................................... 17

7.6 Extended components definition (APE_ECD) .................................................................. 18

7.6.1 Objectives ......................................................................................................................... 18
7.6.2 APE_ECD.1 Extended components definition ................................................................. 18

7.7 Security requirements (APE_REQ) ..................................................................................... 19

7.7.1 Objectives .......................................................................................................................... 19
7.7.2 Component levelling ........................................................................................................... 19
7.7.3 APE_REQ.1 Direct rationale PP-Module security requirements ........................................ 19
7.7.4 APE_REQ.2 Derived security requirements ...................................................................... 20

8 Class ACE: Protection Profile Configuration evaluation .......................................................... 22
8.1 General ........................................................................................................................................ 22

8.2 PP-Module introduction (ACE_INT) ...................................................................................... 22

8.2.1 Objectives .......................................................................................................................... 22
8.2.2 ACE_INT.1 PP-Module introduction .................................................................................. 22

8.3 PP-Module conformance claims (ACE_CCL) .................................................................... 23

8.3.1 Objectives .......................................................................................................................... 23
8.3.2 ACE_CCL.1 PP-Module conformance claims .................................................................. 24

8.4 PP-Module security problem definition (ACE_SPD) .............................................................. 25

8.4.1 Objectives .......................................................................................................................... 25
8.4.2 ACE_SPD.1 PP-Module security problem definition .......................................................... 25

8.5 PP-Module security objectives (ACE_OBJ) ....................................................................... 26

8.5.1 Objectives .......................................................................................................................... 26
8.5.2 Component levelling ........................................................................................................... 26
8.5.3 ACE_OBJ.1 PP-Module security objectives for the operational environment ................. 26
8.5.4 ACE_OBJ.2 PP-Module security objectives ...................................................................... 27

8.6 PP-Module extended components definition (ACE_ECD) ................................................... 27

8.6.1 Objectives .......................................................................................................................... 27
8.6.2 ACE_ECD.1 PP-Module extended components definition ............................................... 28

8.7 PP-Module security requirements (ACE_REQ) ................................................................ 28

8.7.1 Objectives .......................................................................................................................... 28
8.7.2 Component levelling ........................................................................................................... 29
8.7.3 ACE_REQ.1 PP-Module stated security requirements ......................................................... 29
8.7.4 ACE_REQ.2 PP-Module derived security requirements ..................................................... 30

8.8 PP-Module consistency (ACE_MCO) .................................................................................... 31

8.8.1 Objectives .......................................................................................................................... 31
8.8.2 ACE_MCO.1 PP-Module consistency ............................................................................... 31

8.9 PP-Configuration consistency (ACE_CCO) ............................................................................. 32

8.9.1 Objectives .......................................................................................................................... 32
8.9.2 ACE_CCO.1 PP-Configuration consistency ..................................................................... 33

9 Class ASE: Security Target (ST) evaluation ........................................................................... 36
9.1 General ........................................................................................................................................ 36

9.2 ST introduction (ASE_INT) .................................................................................................... 36

9.2.1 Objectives .......................................................................................................................... 36
9.2.2 ASE_INT.1 ST introduction ............................................................................................... 36

9.3 Conformance claims (ASE_CCL) ........................................................................................... 37

9.3.1 Objectives .......................................................................................................................... 37
9.3.2 ASE_CCL.1 Conformance claims ..................................................................................... 38

9.4 Security problem definition (ASE_SPD) .............................................................................. 39

9.4.1 Objectives .......................................................................................................................... 39
9.4.2 ASE_SPD.1 Security problem definition .......................................................................... 39

9.5 Security objectives (ASE_OBJ) ............................................................................................ 40

9.5.1 Objectives .......................................................................................................................... 40
9.5.2 Component levelling ........................................................................................................... 40
9.5.3 ASE_OBJ.1 Security objectives for the operational environment .................................... 40
9.5.4 ASE_OBJ.2 Security objectives ....................................................................................... 41

9.6 Extended components definition (ASE_ECD) ..................................................................... 42
10 Class ADV: Development

10.1 General

10.2 Security Architecture (ADV_ARC)

10.3 Functional specification (ADV_FSP)

10.4 Implementation representation (ADV_IMP)

10.5 TSF internals (ADV_INT)

10.6 Security policy modelling (ADV_SPM)

10.7 TOE design (ADV_TDS)
10.8 Composite design compliance (ADV_COMP) ................................................................. 80
10.8.1 Objectives ........................................................................................................... 80
10.8.2 Component levelling .......................................................................................... 80
10.8.3 Application notes ............................................................................................... 80
10.8.4 ADV_COMP.1 Design compliance with the base component-related user guidance, ETR for composite evaluation and report of the base component evaluation authority ........................................................................... 81

11 Class AGD: Guidance documents .................................................................................. 82
11.1 General .................................................................................................................... 82
11.2 Operational user guidance (AGD_OPE) .................................................................. 82
11.2.1 Objectives .......................................................................................................... 82
11.2.2 Component levelling ......................................................................................... 83
11.2.3 Application notes ............................................................................................... 83
11.2.4 AGD_OPE.1 Operational user guidance ............................................................ 83
11.3 Preparative procedures (AGD_PRE) ...................................................................... 84
11.3.1 Objectives .......................................................................................................... 84
11.3.2 Component levelling ......................................................................................... 84
11.3.3 Application notes ............................................................................................... 84
11.3.4 AGD_PRE.1 Preparative procedures .................................................................. 85

12 Class ALC: Life-cycle support ....................................................................................... 85
12.1 General .................................................................................................................... 85
12.2 CM capabilities (ALC_CMC) ................................................................................. 86
12.2.1 Objectives .......................................................................................................... 86
12.2.2 Component levelling ......................................................................................... 87
12.2.3 Application notes ............................................................................................... 87
12.2.4 ALC_CMC.1 Labelling of the TOE .................................................................... 88
12.2.5 ALC_CMC.2 Use of the CM system ................................................................. 88
12.2.6 ALC_CMC.3 Authorization controls ............................................................... 88
12.2.7 ALC_CMC.4 Production support, acceptance procedures and automation ...... 91
12.2.8 ALC_CMC.5 Advanced support ........................................................................ 93
12.3 CM scope (ALC_CMS) .......................................................................................... 96
12.3.1 Objectives .......................................................................................................... 96
12.3.2 Component levelling ......................................................................................... 96
12.3.3 Application notes ............................................................................................... 97
12.3.4 ALC_CMS.1 TOE CM coverage ...................................................................... 97
12.3.5 ALC_CMS.2 Parts of the TOE CM coverage ................................................ 97
12.3.6 ALC_CMS.3 Implementation representation CM coverage ............................ 98
12.3.7 ALC_CMS.4 Problem tracking CM coverage ................................................ 99
12.3.8 ALC_CMS.5 Development tools CM coverage .............................................. 100
12.4 Delivery (ALC_DEL) ............................................................................................. 101
12.4.1 Objectives ......................................................................................................... 101
12.4.2 Component levelling ......................................................................................... 101
12.4.3 Application notes ............................................................................................... 101
12.4.4 ALC_DEL.1 Delivery procedures .................................................................... 101
12.5 Developer environment security (ALC_DVS) ......................................................... 102
12.5.1 Objectives .......................................................................................................... 102
12.5.2 Component levelling ......................................................................................... 102
12.5.3 Application notes ............................................................................................... 102
12.5.4 ALC_DVS.1 Identification of security controls ............................................... 102
13.3 Depth (ATE_DPT)

13.3.1 Objectives

13.3.2 Component levelling

13.3.3 Application notes

13.4 Functional tests (ATE_FUN)

13.4.1 Objectives

13.4.2 Component levelling

13.4.3 Application notes

13.4.4 ATE_FUN.1 Functional testing
13.4.5 ATE_FUN.2 Ordered functional testing .............................................. 129
13.5 Independent testing (ATE_IND) ......................................................... 130
13.5.1 Objectives .................................................................................... 130
13.5.2 Component levelling .................................................................... 130
13.5.3 Application notes .......................................................................... 130
13.5.4 ATE_IND.1 Independent testing - conformance ............................ 131
13.5.5 ATE_IND.2 Independent testing - sample ...................................... 132
13.5.6 ATE_IND.3 Independent testing - complete .................................... 133
13.6 Composite functional testing (ATE_COMP) ........................................ 134
13.6.1 Objectives .................................................................................... 134
13.6.2 Component levelling .................................................................... 134
13.6.3 Application notes .......................................................................... 134
13.6.4 ATE_COMP.1 Composite product functional testing ....................... 134

14 Class AVA: Vulnerability assessment .................................................... 135
14.1 General .............................................................................................. 135
14.2 Application notes ............................................................................. 135
14.3 Vulnerability analysis (AVA_VAN) ...................................................... 136
14.3.1 Objectives .................................................................................... 136
14.3.2 Component levelling .................................................................... 136
14.3.3 AWA_VAN.1 Vulnerability survey ................................................ 136
14.3.4 AWA_VAN.2 Vulnerability analysis .............................................. 137
14.3.5 AWA_VAN.3 Focused vulnerability analysis ................................. 138
14.3.6 AWA_VAN.4 Methodical vulnerability analysis .............................. 139
14.3.7 AWA_VAN.5 Advanced methodical vulnerability analysis .............. 140
14.4 Composite vulnerability assessment (AVA_COMP) ............................. 141
14.4.1 Objectives .................................................................................... 141
14.4.2 Component levelling .................................................................... 141
14.4.3 Application notes .......................................................................... 142
14.4.4 AWA_COMP.1 Composite product vulnerability assessment .......... 142

15 Class ACO: Composition ...................................................................... 143
15.1 General .............................................................................................. 143
15.2 Composition rationale (ACO_COR) ..................................................... 146
15.2.1 Objectives .................................................................................... 146
15.2.2 Component levelling .................................................................... 146
15.2.3 ACO_COR.1 Composition rationale ............................................. 146
15.3 Development evidence (ACO_DEV) .................................................... 146
15.3.1 Objectives .................................................................................... 146
15.3.2 Component levelling .................................................................... 146
15.3.3 Application notes .......................................................................... 146
15.3.4 ACO_DEV.1 Functional Description ............................................ 147
15.3.5 ACO_DEV.2 Basic evidence of design ......................................... 148
15.3.6 ACO_DEV.3 Detailed evidence of design ..................................... 148
15.4 Reliance of dependent component (ACO_REL) .................................... 149
15.4.1 Objectives .................................................................................... 149
15.4.2 Component levelling .................................................................... 150
15.4.3 Application notes .......................................................................... 150
15.4.4 ACO_REL.1 Basic reliance information ........................................ 150
15.4.5 ACO_REL.2 Reliance information ................................................. 150
15.5 Composed TOE testing (ACO_CTT) ................................................... 151
15.5.1 Objectives .................................................................................... 151
15.5.2 Component levelling .................................................................... 151
15.5.3 Application notes .......................................................................... 151
15.5.4 ACO_CTT.1 Interface testing ...................................................... 152
15.5.5 ACO_CTT.2 Rigorous interface testing ........................................ 153
15.6 Composition vulnerability analysis (ACO_VUL) ................................... 154
15.6.1 Objectives .................................................................................... 154
15.6.2 Component levelling .................................................................... 154
### Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.6.3</td>
<td>Application notes</td>
<td>154</td>
</tr>
<tr>
<td>15.6.4</td>
<td>ACO_VUL.1 Composition vulnerability review</td>
<td>155</td>
</tr>
<tr>
<td>15.6.5</td>
<td>ACO_VUL.2 Composition vulnerability analysis</td>
<td>155</td>
</tr>
<tr>
<td>15.6.6</td>
<td>ACO_VUL.3 Enhanced-Basic Composition vulnerability analysis</td>
<td>156</td>
</tr>
<tr>
<td>Annex A</td>
<td>Development (ADV)</td>
<td>158</td>
</tr>
<tr>
<td>Annex B</td>
<td>Composition (ACO)</td>
<td>178</td>
</tr>
<tr>
<td>Annex C</td>
<td>Cross reference of assurance component dependencies</td>
<td>185</td>
</tr>
<tr>
<td>Bibliography</td>
<td></td>
<td>189</td>
</tr>
</tbody>
</table>
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 or www.iec.ch/members_experts/refdocs).

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. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents) or the IEC list of patent declarations received (see https://patents.iec.ch).

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. In the IEC, see 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.

This fourth edition cancels and replaces the third edition (ISO/IEC 15408-3:2008), which has been technically revised.

The main changes are as follows:

— the terminology has been reviewed and updated;
— the exact conformance type has been incorporated;
— low assurance PPs have been removed and direct rationale PPs have been incorporated;
— PP-Modules and PP-Configurations for modular evaluations have been incorporated;
— multi-assurance evaluation has been incorporated.

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

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 and www.iec.ch/national-committees.

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 (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.

Australia       The Australian Signals Directorate
Canada          Communications Security Establishment
France          Agence Nationale 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
New Zealand     Government Communications Security Bureau
Republic of Korea National Security Research Institute
Spain           Ministerio de Asuntos Económicos y Transformación Digital
Sweden          FMV, Swedish Defence Materiel Administration
United Kingdom  National Cyber Security Centre
United States   The National Security Agency
Introduction

Security assurance components, as defined in this document, are the basis for the security assurance requirements expressed in a Security Assurance Package, Protection Profile (PP), a PP-Module, a PP-Configuration, or a Security Target (ST).

These requirements establish a standard way of expressing the assurance requirements for TOEs. This document catalogues the set of assurance components, families and classes. It also defines evaluation criteria for PPs, PP-Configurations, PP-Modules, and STs.

The audience for this document includes consumers, developers, technical working groups, evaluators of secure IT products and others. ISO/IEC 15408-1:2022, Clause 5 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 may use this document as follows:

a) Consumers, who use this document 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.

b) Developers, who respond to actual or perceived consumer security requirements in constructing a TOE, reference this document when interpreting statements of assurance requirements and determining assurance approaches of TOEs.

c) Evaluators, who use the assurance requirements defined in this document as a mandatory statement of evaluation criteria when determining the assurance of TOEs and when evaluating PPs and STs.

NOTE This document uses bold and italic type in some cases to distinguish terms from the rest of the text. The relationship between components within a family is highlighted using a bolding convention. This convention calls for the use of bold type for all new requirements. For hierarchical components, requirements are presented in bold type when they are enhanced or modified beyond the requirements of the previous component. In addition, any new or enhanced permitted operations beyond the previous component are also highlighted using bold type.

The use of italics indicates text that has a precise meaning. For security assurance requirements the convention is for special verbs relating to evaluation.
Information security, cybersecurity and privacy protection — Evaluation criteria for IT security - —

Part 3:
Security assurance components

1 Scope

This document defines the assurance requirements of the ISO/IEC 15408 series. It includes the individual assurance components from which the evaluation assurance levels and other packages contained in ISO/IEC 15408-5 are composed, and the criteria for evaluation of Protection Profiles (PPs), PP-Configurations, PP-Modules, and Security Targets (STs).

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 15408-5, Information security — Evaluation criteria for IT security — Part 5: Pre-defined packages of security requirements
ISO/IEC 18045:2022, Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Methodology for IT security evaluation
ISO/IEC IEEE 24765, Systems and software engineering — Vocabulary

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 15408-1, ISO/IEC 15408-2, ISO/IEC 15408-4, ISO/IEC 15408-5, ISO/IEC 18045 and ISO/IEC IEEE 24765 and the following apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:
— ISO Online browsing platform: available at https://www.iso.org/obp
— IEC Electropedia: available at https://www.electropedia.org/

3.1 acceptance procedure
procedure followed in order to accept newly created or modified configuration items (3.3) as part of the target of evaluation (TOE), or to move them to the next step of the life-cycle

Note 1 to entry: These procedures identify the roles or individuals responsible for the acceptance and the criteria to be applied in order to decide on the acceptance.