INTERNATIONAL STANDARD

ISO/IEC 15408-1

Fourth edition
2022-08

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

Part 1: Introduction and general model

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

Partie 1: Introduction et modèle général

Reference number
ISO/IEC 15408-1:2022(E)

© ISO/IEC 2022

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2022

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 2022 – All rights reserved

Contents

Page

Foreword ... **vi**
Introduction ... **viii**
1 Scope ... **1**
2 Normative references ... **1**
3 Terms and definitions ... **2**
4 Abbreviated terms ... **13**
5 Overview ... **15**
5.1 General ... 15
5.2 ISO/IEC 15408 series description ... 15
5.2.1 General ... 15
5.2.2 Audience ... 16
5.3 Target of evaluation (TOE) ... 19
5.3.1 General ... 19
5.3.2 TOE boundaries ... 19
5.3.3 Different representations of the TOE ... 20
5.3.4 Different configurations of the TOE ... 20
5.3.5 Operational environment of the TOE ... 20
5.4 Presentation of material in this document ... 21
6 General model ... **21**
6.1 Background ... 21
6.2 Assets and security controls ... 21
6.3 Core constructs of the paradigm of the ISO/IEC 15408 series ... 24
6.3.1 General ... 24
6.3.2 Conformance types ... 24
6.3.3 Communicating security requirements ... 24
6.3.4 Meeting the needs of consumers (risk owners) ... 27
7 Specifying security requirements ... **29**
7.1 Security problem definition (SPD) ... 29
7.1.1 General ... 29
7.1.2 Threats ... 29
7.1.3 Organizational security policies (OSPs) ... 30
7.1.4 Assumptions ... 30
7.2 Security objectives ... 31
7.2.1 General ... 31
7.2.2 Security objectives for the TOE ... 31
7.2.3 Security objectives for the operational environment ... 31
7.2.4 Relation between security objectives and the SPD ... 32
7.2.5 Tracing between security objectives and the SPD ... 32
7.2.6 Providing a justification for the tracing ... 33
7.2.7 On countering threats ... 33
7.2.8 Security objectives: conclusion ... 33
7.3 Security requirements ... 33
7.3.1 General ... 33
7.3.2 Security Functional Requirements (SFRs) ... 34
7.3.3 Security assurance requirements (SARs) ... 36
7.3.4 Security requirements: conclusion ... 37
8 Security components ... **38**
8.1 Hierarchical structure of security components ... 38
8.1.1 General ... 38
8.1.2 Class ... 38
8.1.3 Family ... 39

© ISO/IEC 2022 – All rights reserved