

TECHNICAL REPORT

**ISO/IEC
TR
19791**

First edition
2006-05-15

Information technology — Security techniques — Security assessment of operational systems

*Technologies de l'information — Techniques de sécurité — Évaluation
de la sécurité des systèmes opérationnels*

Reference number
ISO/IEC TR 19791:2006(E)



© ISO/IEC 2006

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.

© ISO/IEC 2006

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.....	v
Introduction	vi
1 Scope	1
2 Normative references	1
3 Terms and definitions.....	2
4 Abbreviated terms	4
5 Structure of this Technical Report.....	4
6 Technical approach	5
6.1 The nature of operational systems	5
6.2 Establishing operational system security.....	5
6.3 Security in the operational system life cycle.....	7
6.4 Relationship to other systems	9
7 Extending ISO/IEC 15408 evaluation concepts to operational systems	9
7.1 Overview	9
7.2 General philosophy	9
7.3 Operational system assurance.....	11
7.4 Composite operational systems	13
7.5 Types of security controls	16
7.6 System security functionality.....	17
7.7 Timing of evaluation	18
7.8 Use of evaluated products	19
7.9 Documentation requirements.....	20
7.10 Testing activities.....	20
7.11 Configuration management	21
8 Relationship to existing security standards	22
8.1 Overview	22
8.2 Relationship to ISO/IEC 15408.....	23
8.3 Relationship to non-evaluation standards.....	24
8.4 Relationship to Common Criteria development	24
9 Evaluation of operational systems	24
9.1 Introduction	24
9.2 Evaluation roles and responsibilities	24
9.3 Risk assessment and determination of unacceptable risks	26
9.4 Security problem definition	27
9.5 Security objectives	27
9.6 Security requirements	27
9.7 The system security target (SST).....	29
9.8 Periodic reassessment.....	31
Annex A (normative) Operational system Protection Profiles and Security Targets.....	32
A.1 Specification of System Security Targets.....	32
A.2 Specification of System Protection Profiles	39
Annex B (normative) Operational system functional control requirements	46
B.1 Introduction	46
B.2 Class FOD: Administration	48
B.3 Class FOS: IT systems	56
B.4 Class FOA: User Assets.....	66