



**USING**  
**the**  
**COMMON**  
**CRITERIA**  
**for**

**IT**  
**SECURITY**  
**EVALUATION**

**DEBRA S. HERRMANN**

**USING**  
**the**  
**COMMON**  
**CRITERIA**  
**for**  
**IT**  
**SECURITY**  
**EVALUATION**

---

## OTHER AUERBACH PUBLICATIONS

### **The ABCs of IP Addressing**

Gilbert Held

ISBN: 0-8493-1144-6

### **The ABCs of TCP/IP**

Gilbert Held

ISBN: 0-8493-1463-1

### **Building an Information Security Awareness Program**

Mark B. Desman

ISBN: 0-8493-0116-5

### **Building a Wireless Office**

Gilbert Held

ISBN: 0-8493-1271-X

### **The Complete Book of Middleware**

Judith Myerson

ISBN: 0-8493-1272-8

### **Computer Telephony Integration, 2nd Edition**

William A. Yarberry, Jr.

ISBN: 0-8493-1438-0

### **Cyber Crime Investigator's Field Guide**

Bruce Middleton

ISBN: 0-8493-1192-6

### **Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes**

Albert J. Marcella and Robert S. Greenfield, Editors

ISBN: 0-8493-0955-7

### **Global Information Warfare: How Businesses, Governments, and Others Achieve Objectives and Attain Competitive Advantages**

Andy Jones, Gerald L. Kovachik, and Perry G. Luzwick

ISBN: 0-8493-1114-4

### **Information Security Architecture**

Jan Killmeyer Tudor

ISBN: 0-8493-9988-2

### **Information Security Management Handbook, 4th Edition, Volume 1**

Harold F. Tipton and Micki Krause, Editors

ISBN: 0-8493-9829-0

### **Information Security Management Handbook, 4th Edition, Volume 2**

Harold F. Tipton and Micki Krause, Editors

ISBN: 0-8493-0800-3

### **Information Security Management Handbook, 4th Edition, Volume 3**

Harold F. Tipton and Micki Krause, Editors

ISBN: 0-8493-1127-6

### **Information Security Management Handbook, 4th Edition, Volume 4**

Harold F. Tipton and Micki Krause, Editors

ISBN: 0-8493-1518-2

### **Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management**

Thomas R. Peltier

ISBN: 0-8493-1137-3

### **Information Security Risk Analysis**

Thomas R. Peltier

ISBN: 0-8493-0880-1

### **A Practical Guide to Security Engineering and Information Assurance**

Debra Herrmann

ISBN: 0-8493-1163-2

### **The Privacy Papers: Managing Technology and Consumers, Employee, and Legislative Action**

Rebecca Herold

ISBN: 0-8493-1248-5

### **Secure Internet Practices: Best Practices for Securing Systems in the Internet and e-Business Age**

Patrick McBride, Jody Patilla, Craig Robinson, Peter Thermos, and Edward P. Moser

ISBN: 0-8493-1239-6

### **Securing and Controlling Cisco Routers**

Peter T. Davis

ISBN: 0-8493-1290-6

### **Securing E-Business Applications and Communications**

Jonathan S. Held and John R. Bowers

ISBN: 0-8493-0963-8

### **Securing Windows NT/2000: From Policies to Firewalls**

Michael A. Simonyi

ISBN: 0-8493-1261-2

### **Six Sigma Software Development**

Christine B. Tayntor

ISBN: 0-8493-1193-4

### **A Technical Guide to IPsec Virtual Private Networks**

James S. Tiller

ISBN: 0-8493-0876-3

### **Telecommunications Cost Management**

Brian DiMarsico, Thomas Phelps IV, and William A. Yarberry, Jr.

ISBN: 0-8493-1101-2

## AUERBACH PUBLICATIONS

[www.auerbach-publications.com](http://www.auerbach-publications.com)

To Order Call: 1-800-272-7737 • Fax: 1-800-374-3401

E-mail: [orders@crcpress.com](mailto:orders@crcpress.com)

**USING**  
the  
**COMMON**  
**CRITERIA**  
for  
**IT**  
**SECURITY**  
**EVALUATION**

---

**DEBRA S. HERRMANN**



**AUERBACH PUBLICATIONS**

---

A CRC Press Company

Boca Raton London New York Washington, D.C.

### Library of Congress Cataloging-in-Publication Data

Herrmann, Debra S.

Using the Common Criteria for IT security evaluation / Debra S. Herrmann.

p. cm.

Includes bibliographical references and index.

ISBN 0-8493-1404-6 (alk. paper)

1. Telecommunication—Security measures—Standards. 2. Computer security—Standards. 3. Information technology—Standards. I. Title.

TK5102.85 .H47 2002

005.8—dc21

2002033250

CIP

This book contains information obtained from authentic and highly regarded sources. Reprinted material is quoted with permission, and sources are indicated. A wide variety of references are listed. Reasonable efforts have been made to publish reliable data and information, but the author and the publisher cannot assume responsibility for the validity of all materials or for the consequences of their use.

Neither this book nor any part may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, microfilming, and recording, or by any information storage or retrieval system, without prior permission in writing from the publisher.

The consent of CRC Press LLC does not extend to copying for general distribution, for promotion, for creating new works, or for resale. Specific permission must be obtained in writing from CRC Press LLC for such copying.

Direct all inquiries to CRC Press LLC, 2000 N.W. Corporate Blvd., Boca Raton, Florida 33431.

**Trademark Notice:** Product or corporate names may be trademarks or registered trademarks, and are used only for identification and explanation, without intent to infringe.

**Visit the Auerbach Publications Web site at [www.auerbach-publications.com](http://www.auerbach-publications.com)**

© 2003 by CRC Press LLC

Auerbach is an imprint of CRC Press LLC

No claim to original U.S. Government works

International Standard Book Number 0-8493-1404-6

Library of Congress Card Number 2002033250

Printed in the United States of America 1 2 3 4 5 6 7 8 9 0

Printed on acid-free paper

---

# Dedication

---

This book is dedicated to the victims of terrorist attacks  
in Israel, New York City, Pennsylvania, and Washington, D.C.



---

# Other Books by the Author

---

*A Practical Guide to Security Engineering and Information Assurance* (Auerbach Publications, 2001)

*Software Safety and Reliability: Techniques, Approaches and Standards of Key Industrial Sectors* (IEEE Computer Society Press, 1999)





---

# Table of Contents

---

<i>List of Exhibits</i> .....	xiii
-------------------------------	------

<b>Chapter 1 Introduction</b> .....	1
-------------------------------------	---

1.0 Background .....	1
1.1 Purpose .....	2
1.2 Scope .....	2
1.3 Intended Audience .....	2
1.4 Organization .....	2

<b>Chapter 2 What Are the Common Criteria? .....</b>	<b>5</b>
--	----------

2.0 History .....	5
2.1 Purpose and Intended Use .....	10
2.2 Major Components of the Methodology and How They Work .....	12
2.2.1 The CC .....	12
2.2.2 The CEM .....	32
2.3 Relationship to Other Standards .....	33
2.4 CC User Community and Stakeholders .....	44
2.5 Future of the CC .....	47
2.6 Summary .....	54
2.7 Discussion Problems .....	56

<b>Chapter 3 Specifying Security Requirements: The Protection Profile .....</b>	<b>57</b>
---	-----------

3.0 Purpose .....	57
3.1 Structure .....	60
3.2 Section 1: Introduction .....	62
3.2.1 PP Identification .....	63
3.2.2 PP Overview .....	63
3.3 Section 2: TOE Description .....	67
3.3.1 General Functionality .....	67
3.3.2 TOE Boundaries .....	70
3.4 Section 3: TOE Security Environment .....	73
3.4.1 Assumptions .....	73

3.4.2 Threats .....	74
3.4.3 Organizational Security Policies .....	76
3.5 Section 4: Security Objectives .....	79
3.6 Section 5: Security Requirements .....	86
3.6.1 Security Functional Requirements (SFRs) .....	89
3.6.2 Security Assurance Requirements (SARs) .....	105
3.6.3 Security Requirements for the IT Environment .....	113
3.6.4 Security Requirements for the Non-IT Environment .....	117
3.7 Section 6: PP Application Notes .....	118
3.8 Section 7: Rationale .....	118
3.8.1 Security Objectives Rationale .....	119
3.8.2 Security Requirements Rationale .....	120
3.9 Summary .....	121
3.10 Discussion Problems .....	123

## **Chapter 4 Designing a Security Architecture: The Security Target ..... 125**

4.0 Purpose .....	125
4.1 Structure .....	127
4.2 Section 1: Introduction .....	131
4.2.1 ST Identification .....	131
4.2.2 ST Overview .....	132
4.3 Section 2: TOE Description .....	133
4.3.1 System Type .....	134
4.3.2 Architecture .....	134
4.3.3 Security Boundaries .....	135
4.4 Section 3: Security Environment .....	136
4.4.1 Assumptions .....	136
4.4.2 Threats .....	138
4.4.3 Organizational Security Policies .....	139
4.5 Section 4: Security Objectives .....	139
4.6 Section 5: Security Requirements .....	142
4.6.1 Security Functional Requirements (SFRs) .....	142
4.6.2 Security Assurance Requirements (SARs) .....	147
4.6.3 Security Requirements for the IT Environment .....	147
4.6.4 Security Requirements for the Non-IT Environment .....	149
4.7 Section 6: Summary Specification .....	150
4.7.1 TOE Security Functions .....	150
4.7.2 Security Assurance Measures .....	155
4.8 Section 7: PP Claims .....	156
4.8.1 PP Reference .....	156
4.8.2 PP Tailoring .....	158
4.8.3 PP Additions .....	158
4.9 Section 8: Rationale .....	158
4.9.1 Security Objectives Rationale .....	160
4.9.2 Security Requirements Rationale .....	160
4.9.3 TOE Summary Specification Rationale .....	167
4.9.4 PP Claims Rationale .....	169
4.10 Summary .....	170
4.11 Discussion Problems .....	173

<b>Chapter 5 Verifying a Security Solution: Security Assurance Activities .....</b>	<b>175</b>
5.0 Purpose .....	175
5.1 ISO/IEC 15408-3 .....	178
5.1.1 EALs .....	179
5.1.2 PP Evaluation .....	200
5.1.3 ST Evaluation .....	202
5.1.4 TOE Evaluation .....	204
5.1.5 Maintenance of Assurance Evaluation .....	206
5.2 Common Evaluation Methodology (CEM) .....	209
5.3 National Evaluation Schemes .....	217
5.4 Interpretation of Results .....	225
5.5 Relation to Security Certification and Accreditation Activities (C&A) .....	228
5.6 Summary .....	232
5.7 Discussion Problems .....	233
<b>Chapter 6 Postscript.....</b>	<b>235</b>
6.0 ASE: Security Target Evaluation .....	235
6.1 AVA: Vulnerability Analysis and Penetration Testing .....	236
6.2 Services Contracts .....	237
6.3 Schedules for New CC Standards (ISO/IEC and CCIMB) .....	237
<b>Annex A: Glossary of Acronyms and Terms .....</b>	<b>239</b>
<b>Annex B: Additional Resources .....</b>	<b>253</b>
Standards, Regulations, and Policy .....	253
Historical .....	253
Current .....	254
Publications .....	257
Online Resources .....	258
<b>Annex C: Common Criteria Recognition Agreement (CCRA) Participants .....</b>	<b>261</b>
Australia and New Zealand .....	262
Canada .....	262
Finland.....	262
France.....	263
Germany.....	263
Greece .....	263
Israel .....	263
Italy .....	264
The Netherlands .....	264
Norway .....	264
Spain.....	264
Sweden .....	265
United Kingdom .....	265
United States .....	265

<b>Annex D: Accredited Common Criteria Testing Labs .....</b>	<b>267</b>
Australia and New Zealand .....	267
Canada.....	268
France.....	269
Germany.....	270
United Kingdom .....	271
United States .....	273
<b>Annex E: Accredited Cryptographic Module Testing Laboratories.....</b>	<b>275</b>
Canada.....	275
United States .....	276
<b>Annex F: Glossary of Classes and Families .....</b>	<b>279</b>
<b>Index.....</b>	<b>283</b>

---

# List of Exhibits

---

## Chapter 2

<b>Exhibit 1.</b>	Time Line of Events Leading to the Development of the CC .....	6
<b>Exhibit 2.</b>	Summary of <i>Orange Book</i> Trusted Computer System Evaluation Criteria (TCSEC) Divisions.....	8
<b>Exhibit 3.</b>	Major Components of the CC/CEM.....	13
<b>Exhibit 4.</b>	Relationship between PPs, STs, and TOEs.....	15
<b>Exhibit 5.</b>	Relationship between Classes, Families, Components, and Elements...	15
<b>Exhibit 6.</b>	Functional Security Classes .....	16
<b>Exhibit 7.</b>	FAU Functional Class: Security Audit.....	19
<b>Exhibit 8.</b>	FCO Functional Class: Communication.....	19
<b>Exhibit 9.</b>	FCS Functional Class: Cryptographic Support .....	20
<b>Exhibit 10.</b>	FDP Functional Class: User Data Protection .....	21
<b>Exhibit 11.</b>	FIA Functional Class: Identification and Authentication.....	23
<b>Exhibit 12.</b>	FMF Functional Class: Security Management .....	24
<b>Exhibit 13.</b>	FPR Functional Class: Privacy.....	25
<b>Exhibit 14.</b>	FPT Functional Class: Protection of the TSF.....	26
<b>Exhibit 15.</b>	FRU Functional Class: Resource Utilization.....	28
<b>Exhibit 16.</b>	FTA Functional Class: TOE Access.....	28
<b>Exhibit 17.</b>	FTP Functional Class: Trusted Path/Channels .....	29
<b>Exhibit 18.</b>	Standard Notation for Functional Classes, Families, Components, and Elements .....	29
<b>Exhibit 19.</b>	Security Assurance Classes .....	30
<b>Exhibit 20.</b>	APE Assurance Class: Protection Profile Evaluation .....	32
<b>Exhibit 21.</b>	ASE Assurance Class: Security Target Evaluation.....	33
<b>Exhibit 22.</b>	ACM Assurance Class: Configuration Management.....	34
<b>Exhibit 23.</b>	ADO Assurance Class: Delivery and Operation.....	34
<b>Exhibit 24.</b>	ADV Assurance Class: Development.....	35
<b>Exhibit 25.</b>	AGD Assurance Class: Guidance Documents .....	36
<b>Exhibit 26.</b>	ALC Assurance Class: Lifecycle Support .....	37
<b>Exhibit 27.</b>	ATE Assurance Class: Tests.....	38
<b>Exhibit 28.</b>	AVA Assurance Class: Vulnerability Assessment .....	39
<b>Exhibit 29.</b>	AMA Assurance Class: Maintenance of Assurance .....	40
<b>Exhibit 30.</b>	Standard Notation for Assurance Classes, Families, Components, and Elements.....	40

<b>Exhibit 31.</b> Standard EAL Packages .....	41
<b>Exhibit 32.</b> Relationship of the CC/CEM to Other Standards .....	42
<b>Exhibit 33.</b> Roles and Responsibilities of CC/CEM Stakeholders .....	45
<b>Exhibit 34.</b> Interaction among Major CC/CEM Stakeholders .....	48
<b>Exhibit 35.</b> RI Process .....	49
<b>Exhibit 36.</b> CCIMB Final Interpretations .....	50

## Chapter 3

<b>Exhibit 1.</b> Mapping of CC/CEM Artifacts to Generic System Lifecycle and Procurement Phases .....	60
<b>Exhibit 2.</b> Content of a Protection Profile (PP) .....	61
<b>Exhibit 3.</b> Interaction among Sections of a PP .....	62
<b>Exhibit 4.</b> PP Identification Examples .....	64
<b>Exhibit 5.</b> PP Overview Examples .....	65
<b>Exhibit 6.</b> PP Organization Example .....	66
<b>Exhibit 7.</b> Comparison of Information Captured by CCRA PP Registries and the ISO/IEC JTC 1 Registration Authority .....	67
<b>Exhibit 8.</b> TOE Description Examples .....	68
<b>Exhibit 9.</b> Asset Identification: Step 1 .....	70
<b>Exhibit 10.</b> Asset Identification: Step 2 .....	71
<b>Exhibit 11.</b> TOE Boundary Definition Example .....	72
<b>Exhibit 12.</b> TOE Boundary Definition Example .....	73
<b>Exhibit 13.</b> PP Assumptions Example .....	75
<b>Exhibit 14.</b> Threat Assessment: Step 1 .....	77
<b>Exhibit 15.</b> Threat Assessment: Step 2 .....	80
<b>Exhibit 16.</b> Sample Organizational Security Policies .....	84
<b>Exhibit 17.</b> Chronology of Threat Control Measures .....	86
<b>Exhibit 18.</b> Priorities for Preventing Security Vulnerabilities .....	87
<b>Exhibit 19.</b> Sample Security Objectives for TOE .....	87
<b>Exhibit 20.</b> Sample Security Objectives for the Environment .....	88
<b>Exhibit 21.</b> Selection of Security Functional Requirements .....	90
<b>Exhibit 22.</b> Security Functional Requirements (SFRs) Mapped to Security Objectives .....	91
<b>Exhibit 23.</b> Functional Hierarchy Example .....	96
<b>Exhibit 24.</b> Functional Dependencies .....	97
<b>Exhibit 25.</b> Selection of Security Assurance Requirements .....	106
<b>Exhibit 26.</b> Assurance Components That Are Not a Member of an EAL Assurance Package .....	108
<b>Exhibit 27.</b> Security Assurance Requirements (SARs) Mapped to Security Objectives .....	112
<b>Exhibit 28.</b> Assurance Dependencies .....	114
<b>Exhibit 29.</b> PP Application Notes Example .....	119
<b>Exhibit 30.</b> Sample Security Objectives Rationale .....	121
<b>Exhibit 31.</b> Sample Security Requirements Rationale .....	122

## Chapter 4

<b>Exhibit 1.</b> Mapping of CC/CEM Artifacts to Generic System Lifecycle and Procurement Phases .....	128
<b>Exhibit 2.</b> Content of a Security Target (ST) .....	129
<b>Exhibit 3.</b> Interaction Among Section of an ST .....	131
<b>Exhibit 4.</b> Similarities and Differences between Sections in a PP and Sections in an ST .....	132

<b>Exhibit 5.</b> Relationship between an ST and a PP for a Composite TOE .....	133
<b>Exhibit 6.</b> ST Identification Examples .....	133
<b>Exhibit 7.</b> ST System Type .....	135
<b>Exhibit 8.</b> ST Architecture Example .....	136
<b>Exhibit 9.</b> TOE Security Boundary Definitions .....	137
<b>Exhibit 10.</b> ST Assumptions .....	138
<b>Exhibit 11.</b> ST Threat Identification .....	140
<b>Exhibit 12.</b> ST Threat Assessment .....	143
<b>Exhibit 13.</b> TOE Summary Specification Mapping .....	147
<b>Exhibit 14.</b> TSF Mapping Example: Step 1 .....	148
<b>Exhibit 15.</b> TSF Structure Example: Step 2 .....	149
<b>Exhibit 16.</b> Mapping Security Mechanisms to TSF Packages: Step 3 .....	152
<b>Exhibit 17.</b> Sample TTSS for Audit Requirements: Step 4 .....	153
<b>Exhibit 18.</b> Sample TSS Strength of Function Criteria: Step 5 .....	154
<b>Exhibit 19.</b> Sample TSS Security Assurance Measures .....	156
<b>Exhibit 20.</b> TSS Security Assurance Mapping .....	157
<b>Exhibit 21.</b> Sample PP Claims .....	159
<b>Exhibit 22.</b> Security Objectives Rationale .....	161
<b>Exhibit 23.</b> Requirements Rationale — SFRs Necessary .....	163
<b>Exhibit 24.</b> Requirements Rationale: Auditable Events .....	164
<b>Exhibit 25.</b> Requirements Rationale: SARs necessary and sufficient .....	164
<b>Exhibit 26.</b> Requirements Rationale: Component Dependency Analysis .....	166
<b>Exhibit 27.</b> Subsection 8.1 of the Rationale .....	168
<b>Exhibit 28.</b> Subsection 8.2 of the Rationale .....	168
<b>Exhibit 29.</b> Subsection 8.3 of the Rationale .....	168
<b>Exhibit 30.</b> Requirements Rationale: TOE SOF Claims .....	169
<b>Exhibit 31.</b> Security Assurance Measures Mapped to SARs .....	169

## Chapter 5

<b>Exhibit 1.</b> Mapping of CC/CEM Artifacts to Generic System Lifecycle and Procurement Phases .....	176
<b>Exhibit 2.</b> Mapping between Vulnerability Sources, Security Assurance Classes, and Evaluation Techniques .....	180
<b>Exhibit 3.</b> EAL 1 Assurance Package .....	181
<b>Exhibit 4.</b> EAL 2 Assurance Package .....	182
<b>Exhibit 5.</b> EAL 3 Assurance Package .....	185
<b>Exhibit 6.</b> EAL 4 Assurance Package .....	187
<b>Exhibit 7.</b> EAL 5 Assurance Package .....	190
<b>Exhibit 8.</b> EAL 6 Assurance Package .....	193
<b>Exhibit 9.</b> EAL 7 Assurance Package .....	196
<b>Exhibit 10.</b> PP Evaluation .....	200
<b>Exhibit 11.</b> ST Evaluation .....	202
<b>Exhibit 12.</b> TOE Evaluation .....	205
<b>Exhibit 13.</b> Maintenance of Assurance Evaluation .....	207
<b>Exhibit 14.</b> Content of an Observation Report (OR) .....	213
<b>Exhibit 15.</b> Content of an Evaluation Technical Report (ETR) .....	214
<b>Exhibit 16.</b> Evaluation Phases (CCEVS)—Phase 1 Preparation .....	219
<b>Exhibit 17.</b> Evaluation Phases (CCEVS): Phase 2 Conduct .....	220
<b>Exhibit 18.</b> Monthly Summary Report Content .....	220
<b>Exhibit 19.</b> Evaluation Phases (CCEVS): Phase 3 Conclusion .....	221
<b>Exhibit 20.</b> Validation Report Content .....	221
<b>Exhibit 21.</b> Content of a Common Criteria Certificate for a Protection Profile (CCEVS) .....	222



<b>Exhibit 22.</b> Content of a Common Criteria Certificate for an IT Product (CCEVS) .....	223
<b>Exhibit 23.</b> Evaluation Phases (CCEVS): Phase 4 Maintenance of Assurance.....	224
<b>Exhibit 24.</b> Timetable for Scheduling CEM Reviews .....	225
<b>Exhibit 25.</b> Incremental Verification Process: CC/CEM through C&A.....	229
<b>Exhibit 26.</b> Comparison between CCC/CEM and NIACAP Evaluation Phases and Artifacts.....	230

# Chapter 1

---

## Introduction

---

### 1.0 Background

In December 1999, ISO/IEC 15408, Parts 1–3 (Criteria for IT Security Evaluation), was approved as an international standard. The Common Criteria (CC) are considered *the* international standard for information technology (IT) security and provide a complete methodology, notation, and syntax for specifying security requirements, designing a security architecture, and verifying the security integrity of an “as built” product, system, or network. Roles and responsibilities for a variety of stakeholders are defined, such as:

- *Customers* — corporations, government agencies, and other organizations who want to acquire security products, systems, and networks
- *Developers* — (a) system integrators who implement or manage security systems and networks for customers, and (b) vendors who manufacture and sell commercial “off the shelf” (COTS) security products
- *Evaluators* — accredited Common Criteria Testing Laboratories, which perform an independent evaluation of the security integrity of a product, system, or network

Many organizations and government agencies require the use of CC-certified products and systems and use the CC methodology in their acquisition process. For example, in the United States, NSTISSP #11 (National Information Assurance Acquisition Policy)<sup>75</sup> mandated the use of CC-evaluated IT security products in critical infrastructure systems starting in July 2002.

Like ISO 9000, the Common Criteria have a mutual recognition agreement so that products certified in one country are recognized in another. As of June 2002, 15 countries have signed the mutual recognition agreement: Australia, Canada, Finland, France, Germany, Greece, Israel, Italy, the Netherlands, New Zealand, Norway, Spain, Sweden, the United Kingdom, and the United States.

## 1.1 Purpose

This book is a user's guide for the Criteria for IT Security Evaluation. It explains in detail how to understand, interpret, apply, and employ the Common Criteria methodology throughout the life of a system, including the acquisition and certification and accreditation (C&A) processes.

## 1.2 Scope

This book is limited to a discussion of ISO/IEC 15408, Parts 1–3 (Criteria for IT Security Evaluation) and how to use the Common Criteria within a generic system-development lifecycle and a generic procurement process. The terminology, concepts, techniques, activities, roles, and responsibilities comprising the Common Criteria methodology are emphasized.

## 1.3 Intended Audience

This book is written for program managers, product development managers, acquisition managers, security engineers, and system engineers responsible for the specification, design, development, integration, test and evaluation, or acquisition of IT security products and systems. A basic understanding of security engineering concepts and terminology is assumed; however, extensive security engineering experience is not expected.

The Common Criteria define three generic categories of stakeholders: customers, developers, and evaluators. In practice, these categories are further refined into customers or end users, IT product vendors, sponsors, Common Criteria Testing Laboratories (CCTLs), National Evaluation Authorities, and the Common Criteria Implementation Management Board (CCIMB). All six perspectives are captured in this book.

## 1.4 Organization

This book is organized into six chapters. Chapter 1 puts the book in context by explaining the purpose for which the book was written. Limitations on the scope of the subject matter of the book, the intended audience for whom the book was written, and the organization of the book are explained.

Chapter 2 introduces the Common Criteria (CC) by:

- Describing the historical events that led to their development
- Delineating the purpose and intended use of the CC and, conversely, situations not covered by the CC
- Explaining the major concepts and components of the CC methodology and how they work

- Illustrating how the CC relate to other well-known national and international standards
- Discussing the CC user community and stakeholders
- Looking at the future of the CC

Chapter 3 explains how to express security requirements through the instrument of a Protection Profile (PP) using the CC standardized methodology, syntax, and notation. The required content and format of a PP are discussed section by section. The perspective from which to read and interpret PPs is defined. In addition, the purpose, scope, and development of a PP are mapped to both a generic system lifecycle and a generic procurement process.

Chapter 4 explains how to design a security architecture, in response to a PP, through the instrument of a Security Target (ST) using the CC standardized methodology, syntax, and notation. The required content and format of an ST are discussed section by section. The perspective from which to read and interpret STs is defined. In addition, the purpose, scope, and development of an ST are mapped to both a generic system lifecycle and a generic procurement sequence.

Chapter 5 explains how to verify a security solution, whether a system or COTS product, using the CC/CEM (Common Evaluation Methodology). The conduct of security assurance activities is examined in detail, particularly why, how, when, and by whom these activities are conducted. Guidance is provided on how to interpret the results of security assurance activities. The relationship between these activities and a generic system lifecycle, as well as a generic procurement process, is explained. Finally, the role of security assurance activities during ongoing system operations and maintenance is highlighted.

Chapter 6 explores new and emerging concepts within the CC/CEM that are under discussion within the CC user community. These concepts have not yet been formally incorporated into the standard or methodology but are likely to be so in the near future.

Six informative annexes are also provided. Annex A is a glossary of acronyms and terms related to the Common Criteria. Annex B lists the sources that were consulted during the development of this book and provides pointers to other resources that may be of interest to the reader. Annex B is organized in three parts: (1) standards, regulations, and policy; (2) publications; and (3) online resources. Annex C cites the participants who have signed the Common Criteria Recognition Agreement (CCRA) and provides contact information for each country's National Evaluation Authority. Annex D lists organizations that are currently recognized as certified CCTLs in Australia and New Zealand, Canada, France, Germany, the United Kingdom, and the United States. Annex E lists organizations that are currently certified to operate Cryptographic Module Validation Program (CMVP) laboratories in Canada and the United States. Annex F is a glossary of CC three-character class and family mnemonics.

