DRAFT DRAFT DRAFT DRAFT DRAFT

The Canadian Trusted Computer Product Evaluation Criteria

Version 3.0e

January 1993

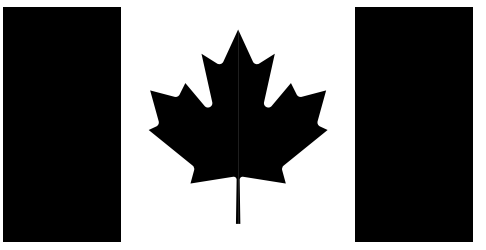
Canadian System Security Centre
Communications Security Establishment
Government of Canada

DRAFT DRAFT DRAFT DRAFT DRAFT

Acknowledgments

Special recognition is extended to the principal authors of the Criteria Working Group at the Communications Security Establishment: Eugen Mate Bačić, CSE (Managing Editor); Aaron Cohen, CSE; Paul Cormier, CSE; Richard Doucette, CSE; Andrew Robison, CSE; and Karin Taylor, CSE. Also due acknowledgment for their input and contributions to this document are William Brierley, CSE; Ken Donaldson, CSE; Milan S. Kuchta, CSE; Gary S. Maxwell, CSE; and Alice Sturgeon, Treasury Board .

Further thanks are offered to the numerous reviewers, both internal to the Communications Security Establishment, and those in industry, government, and various institutions, both at home and internationally, who offered useful comments throughout the development of these criteria. The Canadian Criteria, and the Criteria Working Group, owes much to the caring and enthusiasm shown by the reviewers.



Copyright © 1990, 1991, 1992, 1993 The Government of Canada.

Permission is granted to make and distribute verbatim copies of this document provided the copyright notice and this permission are preserved on all copies.

This document is available in both official languages.

Ce document est disponible en français.

Summary Table of Contents

Foreword xxi

Preface xxiii

Definitions 1

Introduction 11
- Historical Perspective 11
- Scope 12
- Purpose 15
- Structure of the Criteria 15
- Fundamentals 21

Confidentiality Criteria 29
- Covert Channels 29
- Discretionary Confidentiality 30
- Mandatory Confidentiality 32
- Object Reuse 34

Integrity Criteria 35
- Discretionary Integrity 35
- Mandatory Integrity 37
- Physical Integrity 39
- Rollback 41
- Separation of Duties 42
- Self Testing 43

Availability Criteria 45
- Containment 45
- Fault Tolerance 46
- Robustness 47
- Recovery 48

Accountability Criteria 51
- Audit 51
- Identification and Authentication 54
- Trusted Path 55

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

Table of Contents

Assurance Criteria 57
T-0 — Non Compliant 57
Assurance Level T-1 59
Assurance Level T-2 63
Assurance Level T-3 67
Assurance Level T-4 71
Assurance Level T-5 75
Assurance Level T-6 79
Assurance Level T-7 83

Bibliography 87

APPENDICES 89
A Rationale for the Criteria, Services and Levels of Service 91
B Constraints 97
C Fundamentals 105
D Concepts 111
E A Guide to Object Mediation 117
F A Guide to Confidentiality 121
G A Guide to Integrity 131
H A Guide to Availability 147
I A Guide to Accountability 159
J A Guide to Assurance 167
K Implementing Services via Cryptography 179
L Government Security Policy and Standards 189
M Security Functionality Profiles 193

Table of Contents 2

Foreword . . . . . **xxi** 3

Preface . . . . . **xxiii** 4

Definitions **1** 5

Introduction **11** 6

Historical Perspective **11** 7

Scope **12** 8

Functionality 13 9

Assurance 14 10

Evaluation and Rating 14 11

Purpose **15** 12

Structure of the Criteria **15** 13

Levels of Service 18 14

Additional Requirements 19 15

Modifications 19 16

Letter Codes 19 17

Constraints 20 18

Appendices 20 19

Fundamentals **21** 20

Products vs. Systems 21 21

Trusted Computing Bases 21 22

Security Policy 22 23

Isolation, Mediation, & Audit 22 24

Objects 22 25

Object Space 23 26

Tagged Objects 25 27

TCSEC Subjects in the Canadian Criteria 25 28

Continuous Protection 26 29

Security Services & Mechanisms 26 30

Inclusion of New Services 26 31

Modularity 27 32

Composable Evaluations 27 33

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

Table of Contents

Confidentiality Criteria 29

Covert Channels 29

CC–0 Non-compliant 29

CC–1 Covert Channel Analysis 29

CC–2 Auditable Covert Channels 29

CC–3 Elimination of Covert Channels 30

Discretionary Confidentiality 30

CD–0 Non-compliant 30

CD–1 Minimal Discretionary Confidentiality 30

CD–2 Basic Discretionary Confidentiality 31

CD–3 Controlled Discretionary Confidentiality 31

CD–4 Advanced Discretionary Confidentiality 32

Mandatory Confidentiality 32

CM–0 Non-compliant 32

CM–1 Minimal Mandatory Confidentiality 32

CM–2 Basic Mandatory Confidentiality 33

CM–3 Controlled Mandatory Confidentiality 33

CM–4 Advanced Mandatory Confidentiality 34

Object Reuse 34

CR–0 Non-compliant 34

CR–1 Object Reuse 34

Integrity Criteria 35

Discretionary Integrity 35

ID–0 Non-compliant 35

ID–1 Minimal Discretionary Integrity 35

ID–2 Basic Discretionary Integrity 36

ID–3 Controlled Discretionary Integrity 36

ID–4 Advanced Discretionary Integrity 37

Mandatory Integrity 37

IM–0 Non-compliant 37

IM–1 Minimal Mandatory Integrity 37

IM–2 Basic Mandatory Integrity 38

IM–3 Complete Mandatory Integrity 38

IM–4 Advanced Mandatory Integrity 39

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

Table of Contents

Physical Integrity 39
IP–0 Non-compliant 39
IP–1 Basic Physical Integrity 39
IP–2 Intermediate Physical Integrity 40
IP–3 Advanced Physical Integrity 40
IP–4 Complete Physical Integrity 40
Rollback 41
IR–0 Non-compliant 41
IR–1 Restricted Rollback 41
IR–2 Advanced Rollback 41
Separation of Duties 42
IS–0 Non-compliant 42
IS–1 Basic Separation of Duties 42
IS–2 Administrative Separation of Duties 42
IS–3 Privilege-based Separation of Duties 42
Self Testing 43
IT–0 Non-compliant 43
IT–1 Basic Self Testing 43
IT–2 Intermediate Self Testing 43
IT–3 Advanced Self Testing 44

Availability Criteria 45
Containment 45
AC–0 Non-compliant 45
AC–1 Quotas 45
AC–2 Denial of Service 45
AC–3 Resource Restrictions 46
Fault Tolerance 46
AF–0 Non-compliant 46
AF–1 Limited Hot Replacement 46
AF–2 Hot Replacement 46
Robustness 47
AR–0 Non-compliant 47
AR–1 Reliability under Limited Failure 47
AR–2 Reliability with Degraded Service 47
AR–3 Reliability with Full Service 48

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

Table of Contents

Recovery 48
AY–0 Non-compliant 48
AY–1 Manual Recovery 48
AY–2 Automated Recovery 49
AY–3 Selective Recovery 49

Accountability Criteria 51
Audit 51
WA–0 Non-compliant 51
WA–1 External Audit 51
WA–2 Security Audit 52
WA–3 Security Audit & Alarm 52
WA–4 Detailed Audit 53
WA–5 Advanced Detection 53
Identification and Authentication 54
WI–0 Non-compliant 54
WI-1 External I&A 54
WI–2 Individual I&A 54
WI–3 Multiple I&A 55
Trusted Path 55
WT–0 Non-compliant 55
WT–1 Basic Trusted Path 55
WT–2 Advanced Trusted Path 55

Assurance Criteria 57
T-0 — Non Compliant 57
Assurance Level T-1 59
Architecture 59
Development Environment 59
Life Cycle Process. 59
Configuration Management. 59
Development Evidence 59
Functional Specification. 59
Architectural Design. 59
Detailed Design. 60
Operational Environment 60
Security Manuals 60
Security Features User's Guide. 60
Trusted Facility Manual. 60

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

Table of Contents

Security Testing 61

Assurance Level T-2 63

Architecture 63

Development Environment 63

Life Cycle Process. 63

Configuration Management. 63

Development Evidence 63

Functional Specification. 63

Architectural Design. 63

Detailed Design. 64

Operational Environment 64

Security Manuals 64

Security Features User's Guide. 64

Trusted Facility Manual. 64

Security Testing 65

Assurance Level T-3 67

Architecture 67

Development Environment 67

Life Cycle Process. 67

Configuration Management. 67

Development Evidence 68

Functional Specification. 68

Architectural Design. 68

Detailed Design. 68

Operational Environment 69

Security Manuals 69

Security Features User's Guide. 69

Trusted Facility Manual. 69

Security Testing 69

Assurance Level T-4 71

Architecture 71

Development Environment 71

Life Cycle Process. 71

Configuration Management. 71

Development Evidence 72

Functional Specification. 72

Architectural Design. 72

Detailed Design. 72

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

Table of Contents

Operational Environment . . . 73
Security Manuals . . . 73
Security Features User's Guide. . . . 73
Trusted Facility Manual. . . . 73
Security Testing . . . 73
Assurance Level T-5 . . . 75
Architecture . . . 75
Development Environment . . . 75
Life Cycle Process. . . . 75
Configuration Management. . . . 76
Development Evidence . . . 76
Functional Specification. . . . 76
Architectural Design. . . . 76
Detailed Design. . . . 77
Operational Environment . . . 77
Security Manuals . . . 77
Security Features User's Guide. . . . 77
Trusted Facility Manual. . . . 77
Security Testing . . . 78
Assurance Level T-6 . . . 79
Architecture . . . 79
Development Environment . . . 79
Life Cycle Process. . . . 79
Configuration Management. . . . 80
Development Evidence . . . 80
Functional Specification. . . . 80
Architectural Design. . . . 80
Detailed Design. . . . 81
Operational Environment . . . 81
Security Manuals . . . 81
Security Features User's Guide. . . . 81
Trusted Facility Manual. . . . 81
Security Testing . . . 82
Assurance Level T-7 . . . 83
Architecture . . . 83
Development Environment . . . 83
Life Cycle Process. . . . 83
Configuration Management. . . . 84

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

Table of Contents

Development Evidence 84
Functional Specification. 84
Architectural Design. 84
Detailed Design. 85
Operational Environment 85
Security Manuals 85
Security Features User's Guide. 85
Trusted Facility Manual. 85
Security Testing 86

Bibliography 87

APPENDICES 89

A Rationale for the Criteria, Services and Levels of Service 91
Introduction 91
Security Policy 91
Location of Services 92
Tagging 92
Access Matrix 93
CD-1, CM-1, ID-1, and IM-1 94
Confidentiality 94
Discretionary Confidentiality (CD) 94
Mandatory Confidentiality (CM) 94
Object Reuse (OR) 94
Covert Channels (CC) 94
Integrity 95
Discretionary Integrity (CD) 95
Mandatory Integrity (CM) 95
Physical Integrity (IP) 95
Rollback (IR) 95
Separation of Duties (IS) 95
Self Testing (IT) 95
Availability 95
Containment (AC) 95
Fault Tolerance (AF) 95
Robustness (AR) 96
Recovery (AY) 96

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

Table of Contents

Accountability . . . 96
Audit (WA) . . . 96
Identification and Authentication (WI) . . . 96
Trusted Path (WT) . . . 96
Assurance . . . 96

B Constraints . . . 97

Introduction . . . 97
Scope . . . 97
Covert Channels . . . 97
Discretionary Confidentiality . . . 98
Mandatory Confidentiality . . . 99
Discretionary Integrity . . . 99
Mandatory Integrity . . . 100
Rollback . . . 101
Separation of Duties . . . 101
Containment . . . 101
Fault Tolerance . . . 102
Robustness . . . 102
Recovery . . . 103
Audit . . . 103
Trusted Path . . . 104

C Fundamentals . . . 105

Introduction . . . 105
Scope . . . 105
Perspectives . . . 105
Objects . . . 106
Control Over Processes . . . 106
The Reference Monitor . . . 107
Classic View . . . 108
Conclusion . . . 109

D Concepts . . . 111

Introduction . . . 111
Scope . . . 111
The Reference Monitor . . . 111
Encapsulated View . . . 111
Modularity . . . 114
The Overall System . . . 114
The TCB . . . 114
Networks & The Like . . . 116

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

Table of Contents

Conclusion 116

E A Guide to Object Mediation 117

Introduction 117

Scope 117

Tags 117

Discretionary and Mandatory Mediation 118

Accuracy of Tags 119

Creation of New Objects 119

Export and Import of Objects 120

References 120

F A Guide to Confidentiality 121

Introduction 121

Scope 121

Overview of Confidentiality 121

Covert Channels 122

Covert Channel Bandwidths 122

Storage and Timing Channels 122

Aggregate Covert Channels 123

Meeting the Criteria 123

Discretionary Confidentiality 123

Discretionary Security Policy 123

Meeting the Criteria 124

CD-1: Minimal Discretionary Confidentiality 124

CD–2: Basic Discretionary Confidentiality 125

CD–3: Controlled Discretionary Confidentiality 125

CD–4: Advanced Discretionary Confidentiality 126

Mandatory Confidentiality 126

Mandatory Security Policy 126

Meeting the Criteria 126

CM-1: Minimal Mandatory Confidentiality 127

CM–2: Basic Mandatory Confidentiality 128

CM–3: Controlled Mandatory Confidentiality 128

CM–4: Advanced Mandatory Confidentiality 129

Object Reuse 129

Meeting the Criteria 130

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

Table of Contents

References . . . 130
G A Guide to Integrity . . . 131
Introduction . . . 131
Scope . . . 131
Overview of Integrity . . . 131
Discretionary Integrity . . . 132
Security Policy . . . 132
Meeting the Criteria . . . 132
ID-1: Minimal Discretionary Integrity . . . 133
ID–2: Basic Discretionary Integrity . . . 133
ID–3: Controlled Discretionary Integrity . . . 134
ID–4: Advanced Discretionary Integrity . . . 134
Mandatory Integrity . . . 134
Security Policy . . . 134
Meeting the Criteria . . . 135
IM-1: Minimal Mandatory Integrity . . . 136
IM–2: Basic Mandatory Integrity . . . 136
IM–3: Complete Mandatory Integrity . . . 136
IM–4: Advanced Mandatory Integrity . . . 137
Physical Integrity . . . 137
Security Policy . . . 137
Meeting the Criteria . . . 138
IP-1: Basic Physical Integrity . . . 139
IP-2: Intermediate Physical Integrity . . . 139
IP-3: Advanced Physical Integrity . . . 139
IP-4: Complete Physical Integrity . . . 140
Rollback . . . 140
Security Policy . . . 140
Meeting the Criteria . . . 140
IR-1: Restricted Rollback . . . 141
IR-2: Advanced Rollback . . . 141
Separation of Duties . . . 142
Security Policy . . . 142
Meeting the Criteria . . . 142
IS-1: Basic Separation of Duties . . . 143
IS-2: Administrative Separation of Duties . . . 143
IS-3: Privilege-based Separation of Duties . . . 144

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

Table of Contents

Self Testing 144
Security Policy 144
Meeting the Criteria 144
IT-1: Basic Self Testing 145
IT-2: Intermediate Self Testing 145
IT-3: Advanced Self Testing 145
References 145

H A Guide to Availability 147

Introduction 147
Availability Control Objective 147
Scope 147
Requirements for Availability 147
Policies & Issues 148
Models 148
Amoroso Model 149
Yu-Gligor Model 149
CP-6 Quota System 149
Telephone System 151
Perceived Availability 151
Conditioning 152
Testing and Monitoring 152
Common Elements Of The Models 152
Availability Reference Monitor 153
Fault Tolerance 153
Containment 154
Security Policy 154
Meeting the Criteria 154
AC-1: Quotas 154
AC-2: Denial of Service 155
AC-3: Resource Restrictions 155
Fault Tolerance 155
Security Policy 155
Meeting the Criteria 155
AF-1: Limited Hot Replacement 155
AF-2: Hot Replacement 156

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

Table of Contents

Robustness 156
Security Policy 156
Meeting the Criteria 156
AR-1: Reliability under Limited Failure 156
AR-2: Reliability with Degraded Service 156
AR-3: Reliability with Full Service 157
Recovery 157
References 157

I A Guide to Accountability 159
Introduction 159
Scope 159
Audit 159
General Concerns 159
Effective Auditing. 159
Physical Storage of Audit Data. 160
Meeting the Criteria 160
Audit Granularity. 160
Audit File Analysis. 161
Selection of Audit Events. 161
Active Monitoring. 162
Auditable Events 162
Identification & Authentication 164
Authentication 164
“Something you know.” 164
“Something you have.” 165
“Something you are.” 165
Meeting the Criteria 165
References 166

J A Guide to Assurance 167
Introduction 167
Scope 167
Architecture 167
Development Environment 167
Life Cycle Process 167
Configuration Management 168
Basic Principles. 168
Planning A Configuration Management System. 169
Meeting the Criteria. 170

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

Table of Contents

Development Evidence 171

Terminology 171

Specification Style. 171

Level of Detail. 172

Mapping Requirements. 174

Functional Specification 175

Architectural Design 175

Detailed Design 176

Security Manuals 176

Security Testing 176

Trusted Distribution & Generation 177

References 177

K Implementing Services via Cryptography 179

Introduction 179

Scope 179

Export Controls 180

Scope 180

Security Policy 181

Implementing Services 182

Discretionary Confidentiality 182

Mandatory Confidentiality 183

Object Reuse 183

Identification & Authentication 183

Trusted Path 184

Discretionary Integrity 184

Mandatory Integrity 184

Separation of Duties 184

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

Table of Contents

Integration 185
References 187

L Government Security Policy and Standards 189

Introduction 189
Objective & Scope 190
Security Policy Considerations 190
Accountability, Risk, and Guidance 191
Applying the Policy (In Brief) 191

M Security Functionality Profiles 193

Introduction 193
Scope 194
Equivalency & Other Criteria 194
Creation of Profiles 195
Profile Semantics 195
Predefined Profiles 197
The TCSEC Profiles 197
Subsystem Profiles 198
Service Specific Architectures 199
The Infinite Nature of Profiles 201

List of Figures

Figure 1 Product Development and Evaluation Processes. 14
Figure 2 Generic Page Outline 16
Figure 3 Odd (Right Hand) Page Format 17
Figure 4 Even (Left Hand) Page Format 18
Figure 5 State Transitions from an Entity to an Object, User, or Process 22
Figure 6 Information Flow Between User, Process, and Object . 23
Figure 7 Interaction Between TCB Controlled Objects 23
Figure 8 Objects and Their Counterparts 24
Figure 9 “Objects” in the TCSEC and the Canadian Criteria . . . 26
Figure 10 Trusted “Objects” in the TCSEC vs. Canadian Criteria . 106
Figure 11 Classic View of a Reference Monitor 108
Figure 12 Reference Monitor As Encapsulator 112
Figure 13 Entity Style (Message Passing) Reference Monitor . . . 113
Figure 14 Modularity within A Trusted Environment 115
Figure 15 User-Process-Object Interrelationship for Object Mediation 124
Figure 16 User-Process-Object Interrelationship for Object Mediation 127
Figure 17 User-Process-Object Interrelationship for Object Mediation 132
Figure 18 User-Process-Object Interrelationship for Object Mediation 135
Figure 19 Confidentiality-related Auditable Events 162
Figure 20 Integrity-related Auditable Events 163
Figure 21 Availability-related Auditable Events 163
Figure 22 Accountability-related Auditable Events 163
Figure 23 Miscellaneous Auditable Events 164
Figure 24 “Stated” Evidence 173
Figure 25 “Described” Evidence 173
Figure 26 “Explained” Evidence 174
Figure 27 Cryptography and Tags in Discretionary Controls. 183
Figure 28 Stand-Alone Cryptographic Modules 186
Figure 29 Embedded Cryptographic Modules 186
Figure 30 Profile Header Example. 196
Figure 31 Profile Examples. 196

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

List of Tables

Table 1	Mapping of Document Divisions From Standard Nomenclature to Criteria	17
Table 2	Criteria Letter Codes	20
Table 3	Sample Access Matrix of User Tags and Object Tags	93
Table 4	Use of Access Matrixes by Services	93
Table 5	Discretionary Confidentiality Ratings Summary	124
Table 6	Mandatory Confidentiality Ratings Summary	127
Table 7	Discretionary Integrity Ratings Summary	133
Table 8	Mandatory Integrity Ratings Summary	135
Table 9	Common Availability Policy Terminology Mapped to the Availability Criteria	148
Table 10	Front End Quotas	150
Table 11	Resource Limit Quotas	150
Table 12	User Authorization File Quotas	151
Table 13	Generic Quotas	153
Table 14	Levels Affected by Cryptography	181
Table 15	Configurations of Cryptographic Modules within a Host	185
Table 16	C2 Equivalent Profile.	197
Table 17	B1 Equivalent Profile.	197
Table 18	B2 Equivalent Profile.	198
Table 19	B3 Equivalent Profile.	198
Table 20	Standard Partition Subsystem	199
Table 21	Strong Identification Subsystem	199
Table 22	Discretionary Based Subsystem	199
Table 23	Audit Architecture	200
Table 24	Partitioned Architecture	200
Table 25	Comparted Mode Workstation Architecture	200

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

Foreword

This document represents the current state of development of the Canadian Trusted Computer Product Evaluation Criteria (CTCPEC or Canadian Criteria). The purpose of this document is to present a set of technical hardware/firmware/software criteria for trusted products which is consistent with the Security Policy of the Government of Canada, the Information Technology Security Standards under development by the Government of Canada and takes into account reciprocity issues with technical criteria of other nations strategically allied with the Government of Canada. Development of the Canadian Criteria has progressed through workshops and discussions with government and industry.

Review, revision and further development, as appropriate, will be on a continuing basis with reissuance of a revised Canadian Criteria on an as needed basis.

Comments and recommendations for further development and revision of this document are welcomed and should be directed to:

Criteria Coordinator
InfoSec Evaluations/S5B
Communications Security Establishment
P. O. Pox 9703 Terminal
Ottawa, Canada
K1G 3Z4
phone: (613) 991-7331
fax: (613) 991-7323
net: criteria@manitou.cse.dnd.ca

Requests for further hardcopies of this document can be directed at the address above. Electronic copies of the Canadian Trusted Computer Product Evaluation Criteria may be anonymously `FTP`ed from:

ftp.cse.dnd.ca

Login as “anonymous” and supply your “userName@site” as the password.

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

Preface

The Canadian Trusted Computer Product Evaluation Criteria, defined in this document, classify products into broad divisions of security protection. The criteria provide a basis for the evaluation of effectiveness of security controls built into automatic data processing products.

The criteria were developed with two objectives in mind:

1. to provide a comparative scale for the evaluation of commercial products; and
2. to provide a basis for the development of specifications for trusted computer products.

Two types of requirements are delineated for trusted processing:

1. specific security service requirements; and
2. assurance requirements.

Some of the assurance requirements enable evaluation personnel to determine if the required features are present and functioning as intended. These criteria are to be applied to the set of components comprising a trusted product and are not necessarily to be applied to each product component individually. Hence, some components of a product may be completely untrusted, while others may be individually evaluated to a lower or higher evaluation class than the trusted product considered as a whole. In trusted products at the high end of the range, the strength of the isolation and mediation mechanisms is such that many of the product components can be completely untrusted.

The assurance requirements can be applied across the entire spectrum of electronic data processing product or application processing environments without special interpretation.

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

Definitions

A

Access

The performance of a TCB defined operation on an object.

Access Matrix

The matrix containing one tag type along each axis and containing the authorized modes of access in each matrix element. For example, the complete user/object matrix contains all current user tags along one axis and all current object tags along the second axis. Each matrix element contains the set of allowed and disallowed modes of access in the matrix elements.

Access Mediation

TCB determination of authorization and whether access should be granted.

Access Mediation Information

The data structures and algorithms associated with an enforcement decision by the TCB in support of a security policy.

Accountability

The process of ensuring that security relevant events in a product are correcly attributable to a user.

Accreditation

The authorization that is granted for the use of an information technology system to process information in its operational environment.

Administrator, Administrative User

A user to whom an administrative role has been assigned, defined by the Separation of Duties (IS) Service.

Approved

A deliverable is considered approved after the evaluation authority has reviewed it and stated that it is acceptable for the purposes of the evaluation.

Definitions

Assurance

The degree of confidence that a product correctly implements the security policy.

Assurance Level

In evaluation criteria, a specific level on a hierarchical scale representing successively increasing confidence that a product implements the security policy.

Authorization

The right by a user or process to obtain a specific type of access to a specific object.

Availability

The property that a product's services are accessible when needed and without undue delay.

B

C

Certification

The comprehensive assessment of the technical and non-technical security features of an information technology system, made in support of accreditation, that establishes the extent to which a system satisfies a specified security policy.

Component

An identifiable and self-contained portion of a product.

Compromise

A violation of the product's security policy.

Confidential Export

The term used to denote the encapsulation of sensitive data by encryption so that it may be transmitted or stored on electronic media which would otherwise be unsuitable for sensitive data.

Confidentiality

The property that information is not made available or disclosed to an unauthorized user process or object.

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

D

Criteria

A metric used for the evaluation of the effectiveness of security services provided by an information technology product.

Delegation

The passing of authorization from one user or process to another as defined in the product's security policy.

Disclosure

The flow of information from an object to a user or process.

Discretionary

Non-administratively controlled. Under a discretionary policy, authorization and delegation do not require administrative intervention.

E

Entity

A generic descriptor used to discuss an object within a product regardless of state.

Evaluated Rating

The rating which a vendors product has achieved in a completed evaluation.

Evaluation

The process of achieving assurance given a security policy, a consistent description of the security functions and a targeted assurance level.

Evaluation Authority

The organization responsible for the control and management of the evaluation program.

Evaluation Facility

The organization responsible for performing evaluations under the direction of the Evaluation Authority. The Evaluation Authority and Evaluation Facility can be the same organization.

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

Definitions

Event

Any action which causes a change in the state of the product.

Export

A flow of information such that the information is no longer under the control of the TCB.

External

Outside of the control of the TCB.

F

Functionality

The totality of the functional services of a product that contributes to security.

G

H

Heterogenous System

Any collection of components or products which do *not* provide a uniform security policy. Also called a *system.*

Homogenous System

Any collection of components or products, by a single vendor or a consortium, taken collectively but providing a uniform security policy and uniform look and feel.

I

Illegal

Unauthorized.

Import

A flow of information such that the information becomes under the control of the TCB.

Individual

An individual is a single user with respect to the TCB. See the definition of User.

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

Information Flow

The movement of information between users, processes, or objects.

Initialization

Setting an object or a product to a known or predefined state.

Internal

Inside of the control of the TCB.

Isolation

J

K

L

Level

See Level of Service.

Level of Service

A defined and measurable requirement for granularity or strength that addresses a specific set of threats. Each level of service provides a better defence against the threats as the levels increase. Levels of service are hierarchial in terms of protection but not necessarily proper subsets in all cases.

Level 0 is reserved as a placeholder for a product which:

- was evaluated as providing a service; and
- failed to meet the requirements of a higher level of service.

Limit

An authorized restriction, or to enforce an authorized restriction.

M

Mandatory

Administratively controlled. Under a mandatory policy, authorization and delegation require administrative intervention.

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

Definitions

Mechanism

The logic or the algorithm that implements a particular service.

Mediation

The enforcement of a security policy.

Modification

The flow of information from a user or a process to an object.

N

O

Object

An encapsulated resource exported by the TCB. A resource which stores or contains information and upon which the TCB enforces mediation[1].

Object Tag

A tag created or associated based upon the identity of an object. An object tag can be attached by the TCB to a user, process or object.

P

Policy

A statement of scope and mechanism of control.

Process

An active entity under the control of the TCB.

Process Tag

A tag created or associated based upon the identity of a process. A process tag can be attached by the TCB to a user, process or object.

Product

The totality of hardware, firmware, software, and documentation offered by a vendor for evaluation.

[1] Ideally the TCB is opaque and the set of all visible resources in a product is equal to the set of all objects exported by the TCB.

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

Q

Protected Object

The set of objects which are included within a security policy and considered under the control of the TCB.

Protection

The enforcement of a security policy.

R

Rating

The totality of the set of service levels and assurance level of a product. See also Target Rating and Evaluated Rating.

Reference Monitor

An abstract machine concept which mediates accesses to objects by users and processses. A reference monitor embodies three principles: completeness (all accesses are mediated), isolation from interference or tampering, and verifiability.

Resource

A primitive entity exported by or existing in the underlying machine. Anything usable or consumable within a product. See also Object.

Responsibility

Delegated authorization.

Restriction

Limits on access or authorization in the enforcement of the product's security policy.

S

Security

The quality or state being protected from uncontrolled losses or effects.

Security Functionality Profile

See Evaluated Rating.

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

Definitions

Security Policy

A set of rules and procedures regulating the use of information including its processing, storage, distribution and presentation.

Security Policy Model

Security Service

A functional grouping rated for its ability to address a defined set of threats. One or more levels of service is defined for each security service.

Session

A period during which a user interacts with the product.

State

Refers to one of the three states an object may be in: user, process, or object.

Storage

An addressable location to which information can be placed and retrieved.

Subject

The TCSEC term for a process or user. It is used interchangeably in the TCSEC for both.

System

See Heterogenous System.

Tag

A term used to describe any access mediation information associated with users, processes, or objects. The association of a tag with an entity may be explicit or implicit. The tag of an entity is part of its encapsulation by the TCB.

Target Rating

The rating which a vendor intends to achieve in an evaluation.

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

TCB Boundary

The scope of control to which the TCB maintains enforcement of the product's security policy.

Trusted Computing Base (TCB)

The elements of a product, including any hardware, firmware and software, involved in enforcing a product's security policy; or those elements involved in enforcing a given service policy when used in relation to a specific service.

U

Unauthorized

Not authorized. See Authorization.

User

An active entity outside of and not constrained by the product's security policy other than in its interactions with the TCB. The TCB will have explicit and implicit assumptions about users and will use these to create an encapsulated abstraction of the actual entity.

User Tag

A tag created or associated based upon the identity of a user. A user tag can be attached by the TCB to a user, process or object.

User Type

????

An active entity outside of and not constrained by the product's security policy other than in its interactions with the TCB. The TCB will have explicit and implicit assumptions about users and will use these to create an encapsulated abstraction of the actual entity.

V

Vendor

The organization offering a product for evaluation and representing the product's interests to the Evaluation Authority.

Violation

Contrary to the product's security policy.

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

W

X

Y

Z

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

Introduction

Historical Perspective

In the late 1960s and early 1970s, Project MAC[2] of the Massachusetts Institute of Technology (MIT) was working on the next generation operating system. At the same time, MITRE was contracted by the National Bureau of Standards (NBS), now the National Institute of Standards and Technology (NIST), to develop a set of criteria against which systems of high trust could be evaluated. Using Project MAC as a base, MITRE, MIT, Bell Laboratories and General Electric (the latter two replaced by Honeywell) set out to design a system which was highly trusted. The project resulted in two products: Multics and the Trusted Computer System Evaluation Criteria.

The Multics (Multiplexed Information and Computing Service) Operating System was used as the testbed for the security concepts being developed by MITRE. Further, the policy implemented by the Multics operating system was dictated by the Department of Defense (DoD) and formalized by D.E. Bell and L.J. LaPadula; it is commonly known as the Bell-LaPadula Model/Policy. This policy is a confidentiality oriented policy which deals with ensuring that sensitive information is not disclosed to unauthorized individuals.

The Trusted Computer System Evaluation Criteria (TCSEC) was a direct outgrowth of the MITRE/NBS project. Project MAC was tasked with ensuring proof-of-concept as well as the feasibility of the security concepts. The TCSEC was finalized in 1983 and released in the now familiar orange cover as CSC-STD-001–83. In 1985, the TCSEC received a minor update and became a DoD standard, DoD 5200.28–STD. It has popularly become known as the Orange Book and has remained unchanged to date.

In August 1988, the Canadian System Security Centre (CSSC) was formed. Its primary tasks were to develop a criteria which would address issues unique to the Government of Canada and to set up a Canadian evaluation capability.

The first version of the Canadian Criteria was released in May 1989. The basic premise of five base criteria creating a duality of functionality and assurance was evident. In December of 1990, version 2.0 was released; in July 1991 version 2.1[3]. Version 2 was the first to adopt the breakdown of the functional criteria into services with levels of strength and the first to be used for evaluations. The experience gained and the flaws discovered during evaluations, along with

[2] Project MAC was a US Government funded research group.

[3] In order to distinguish between the English and French versions, a letter designator was appended after the version number; an 'e' denotes the English version and an 'f' the French.

Scope

comments received from numerous individuals and organizations, were used by the Criteria Working Group to update and improve the Canadian Criteria.

The U.S. Orange Book, or TCSEC, the baseline of computer security evaluations for years, primarily targets multi-user, monolithic mainframe and mini systems. Databases, networks, subsystems, etc. all are brought in line with the Orange Book by various "interpretations" such as the Trusted Database Interpretation (TDI) or the Trusted Network Interpretation (TNI). To avoid the use of interpretations the Canadian Criteria targets a wider range of products such as monolithic systems, multiprocessor systems, databases, subsystems, distributed systems, networked systems, object-oriented systems, and others.

This widened targeting is accomplished by splitting the Criteria into two distinct groups known as the *duality* of functionality and assurance. Functionality consists of Confidentiality, Integrity, Availability, and Accountability Criteria. Assurance consists of the Assurance Criteria. Each of the criteria within the functionality group are more or less independent of one another. The dependencies which do occur between the various services found in the functional criteria are known as constraints.

A product is defined as a collection of functionality services to which a level of assurance is globally applied. The functionality services selected must be a well-defined set[4], with each service's constraints being adhered to; and with each service selected at a specific level of strength. Note that, with minor exceptions[5], there are no functionality/assurance constraints.

The criteria is a metric used for the evaluation of the effectiveness of the security services provided by a product. Each service is a functional grouping defined for its ability to address a set of threats. For example, the Availability Criteria are divided into Containment, Fault Tolerance, Robustness, and Recovery services. Each of these are components of products which provide availability. However, all of the criteria services need not exist within one product.

The Assurance Criteria, on the other hand, reflects the degree of confidence that a product correctly implements its security policy. Assurance is applied across the entire product under evaluation. A product given a T–4 assurance rating has had this level of assurance applied across all the security services within the product.

[4] A functionality *null set* is acceptable (e.g., in a compiler).

[5] Embedded cryptographic devices are handled as special cases and the reader should refer to Appendix K. Covert Channels is a functionality service with a constraint to an assurance level of T-3.

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

Functionality

Scope

The four functionality criteria define services which are general abstractions of the basic building blocks which can be used to define trusted products.

Most products are defined with a specific threat or operating environment in mind. Further, the threats drive the policy that the product will enforce. The policy defined by the product can be abstracted out to one of the four "policy-oriented" criteria.

Confidentiality: Threats centred around disclosure of information to unauthorized parties is a confidentiality issue. Disclosure can range from the release of classified government documents to the movement of banking information between bank loan managers. Whenever there is a requirement for limitations on the release of information, the services to control disclosure will be found under the *Confidentiality Criteria.*

Integrity: Threats centred around modification of information by unauthorized parties are an integrity issue. Modification can range from the modification of sensitive government documents to the sensitivity of the correctness of patient medicinal dosages in a hospital. Whenever there is a requirement for limitations on the modifiability of information, the services to control modification will be found under the *Integrity Criteria.*

Availability: Threats centred around accessibility of host systems is an availability issue. Accessibility can range from protection against denial of service to the requirement that a system have a minimal mean time between failures. Whenever there is a requirement for insuring accessibility of a system, the services to govern the accessibility will be found under the *Availability Criteria.*

Accountability: Threats centred around authorization and audit of access and manipulation of a system or its data is an accountability issue. Accountability concerns can range from ensuring only authorized individuals access a given system to tracking of user actions within a system. Whenever there is a requirement for monitoring or insuring valid access to a system, the corresponding services will be found under the *Accountability Criteria.*

Each service contains levels. A level of service is a defined and measurable requirement for granularity or strength that addresses a specific set of threats. As the level of service increases, a better defence against the threats is provided. Levels of service are hierarchial in terms of protection but are not necessarily

Assurance

proper subsets in all cases. The levels begin at zero (0) and increase towards an "n", where "n" is unique for each service[6].

Assurance is the degree of confidence that the product's security policy is correctly implemented. Assurance is gained through the *development process* and the *evaluation process*. Development process assurance is gained by Vendor actions to promote correctness. The evaluation process contributes to overall assurance through the analysis of evaluation deliverables and other evaluator actions. The division of vendor and evaluation processes is presented in Figure 1.

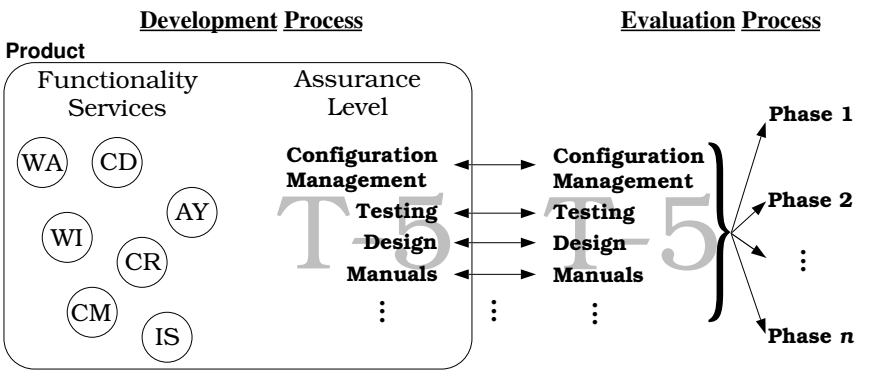


Figure 1: Product Development and Evaluation Processes.

Evaluation and Rating

Each product that enters the evaluation process must have a level of assurance associated with it. The levels of assurance are hierarchical, representing successively increasing confidence that the product security policy is correctly implemented. Greater development and evaluation effort is required as the levels increase.

Evaluation is the process of achieving assurance given a security policy, a consistent description of the security functions and a targeted assurance level. The evaluation results in a rating which is the totality of the set of service levels and assurance level of the product. The ratings of two distinct services, even if their numeric level is the same, do not represent any form of equality.

The evaluated rating will consist of a series of letter-number combinations. These will be grouped by criteria type in the following order: Confidentiality, Integrity, Availability, Accountability and finally Assurance.

[6] For example, the Containment division under the Availability Criteria ranges from AC–0 to AC–3, however the Object Reuse division under the Confidentiality Criteria ranges from CR–0 to CR–1.

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

Purpose

If a product's *target rating* indicates a specific service and service level, failure to meet the service level, or any lower than the target but above zero, would result in a zero level rating. A zero rating is an indication of noncompliance for that particular service. If a product does not implement a particular service, then no rating for that service is given. A zero level rating cannot be specified by a vendor as part of a valid *target rating*.

The criteria have been developed to provide:

1. the Government of Canada with a metric with which to evaluate the degree of assurance that can be placed in computer products used for the processing of sensitive information; and
2. a guide to manufacturers as to what security services to build into their commercial products in order to produce widely available products that satisfy requirements for sensitive applications.
3. a guide which may be used in trusted procurements.

Structure of the Criteria

All Canadian Trusted Computer Product Evaluation Criteria (CTCPEC) releases are denoted by a version number. Each version number is divided into a major and minor release number. A version number is of the form *X.y*, where *X* is the major release number and *y* the minor release number. Whenever substantial changes have occurred to the Criteria[7], the major number will change. For example, from 2 to 3. However, when minor changes occur, such as with editorial corrections, only the minor number is modified, as from 2.0 to 2.1.

The Canadian Trusted Computer Product Evaluation Criteria are organized in a manner allowing for quick reference. Each page of the document is physically divided into four parts: header, footer, subheading column, and text/major headings column (see Figure 2). As Figure 2 indicates, there are also "rapid indices" at the bottom outside corner of each page. These can be used to quickly find the major parts of the Criteria, such as *Introduction, Confidentiality Criteria,* or any of the appendices. Further, Figure 2 presents the flow of the document. The grey arrows indicate the order of the various headings, and implicitly the text associated with each, as found within the Criteria.

The mapping of the standard terms used in addressing portions of a document with those used in the Criteria proper is presented in Table 1. The primary difference is located in the five criteria parts, where chapters are actually the various services defined and the sections are the service levels.

[7] The Criteria is constantly undergoing revision. However, many revisions are minor. On a two year cycle, the Criteria will be reviewed in light of new commentary and changes in industry. If required, a new *major* release of the Criteria will take place. Minor revisions of the Criteria are completed as needed.

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

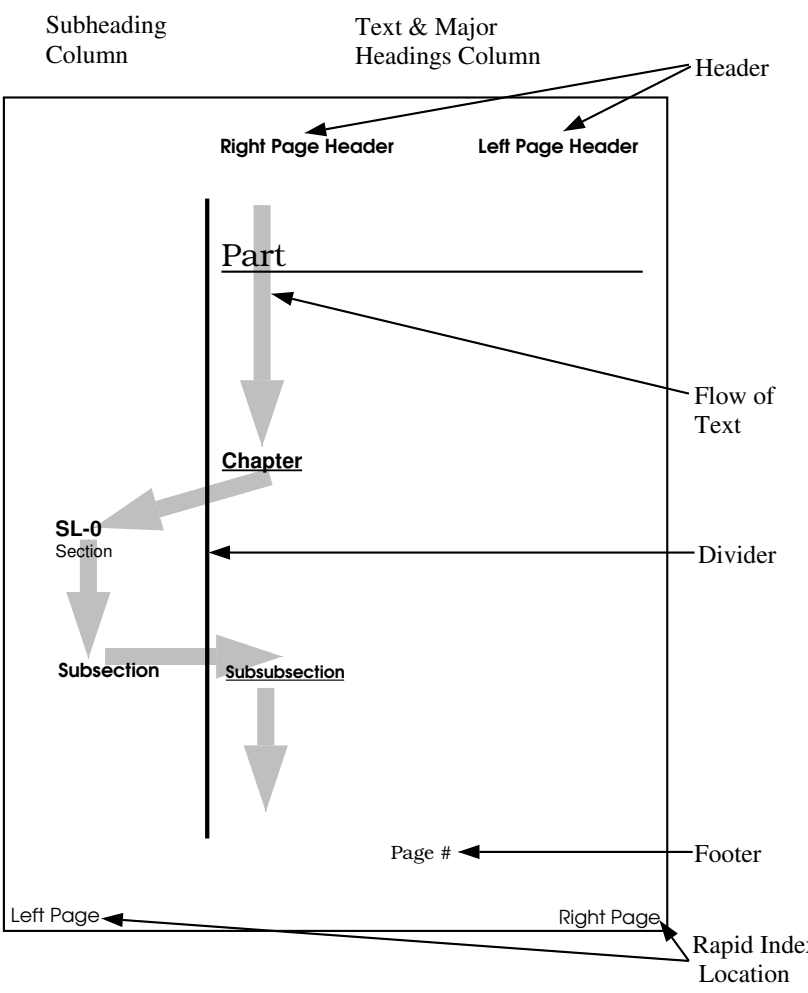


Figure 2: Generic Page Outline 2

By placing the heavily referenced headings as side heads (as illustrated under the "Subheading Column" in Figure 2), they stand out from the rest of the text. This allows the reader to quickly find these sections when referenced in the various appendices or when referenced for evaluation purposes. 3 4 5 6

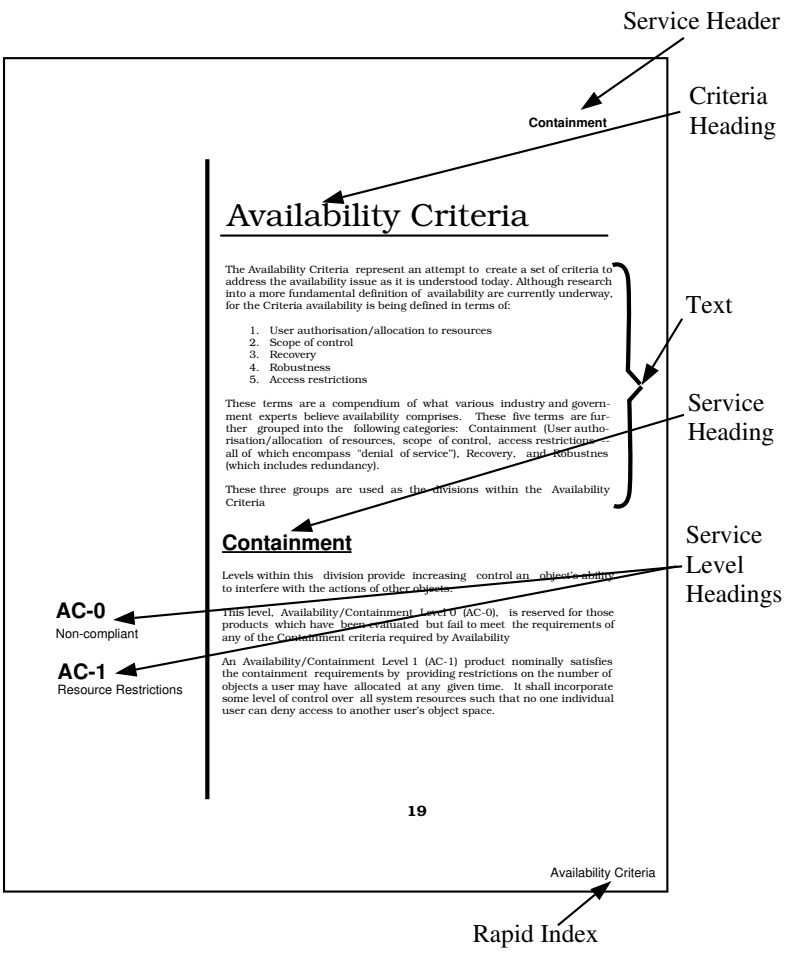


Figure 3: Odd (Right Hand) Page Format

Document Divisions	Definitions Within CTCPEC		
	Introduction	Criteria	Appendices
Part	Introduction	Criteria	n/a
Chapter	Division	Service	Appendix
Section	Section	Service Level	Section
Subsection	Subsection	Subsection	Subsection
Subsubsection	Subsubsection	Subsubsection	Subsubsection

Table 1 Mapping of Document Divisions From Standard Nomenclature to Criteria

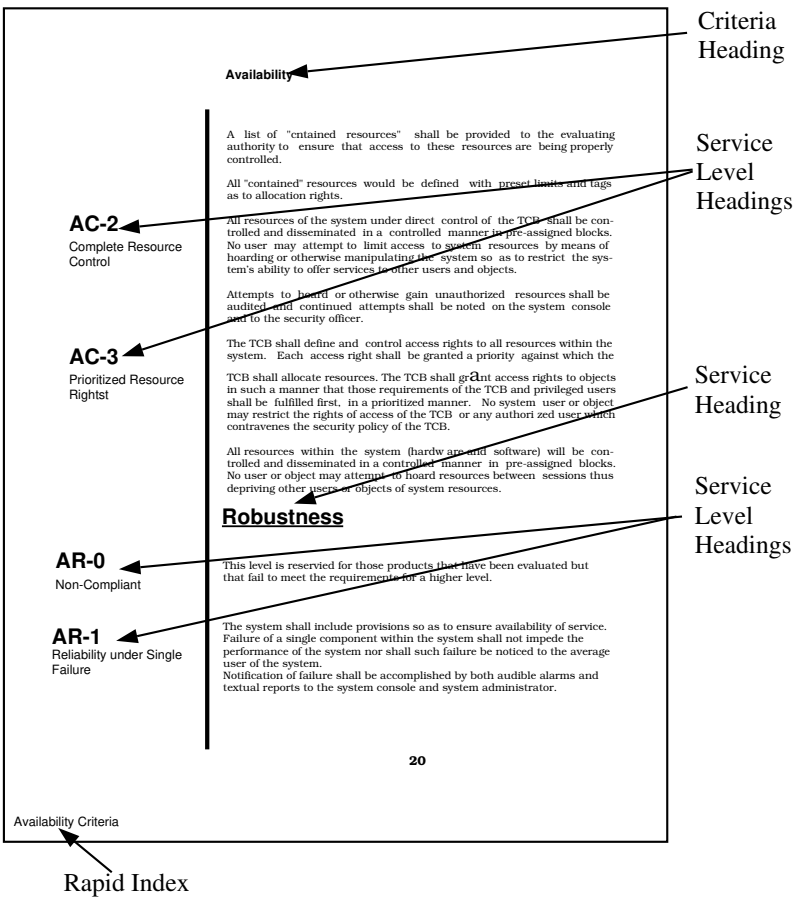


Figure 4: Even (Left Hand) Page Format

More detailed examples of the headings and various pieces which comprise a page within the Criteria are illustrated in Figures 3 and 4.

Levels of Service

Each service level is given as a letter-number combination. Immediately below the level designator is a textual title for the level.

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

Additional Requirements

As the levels of service increase, additional requirements for the new level are **bold faced.**

Modifications

Should minor revisions be necessary, the updated portions of the Criteria would have a change bar along the left side of the modified text, as illustrated for this paragraph. A major revision to the Criteria will **not** contain any change bars.

Letter Codes

With many words beginning with the same letters and the limit of 26 letters, some compromises were made. The following list contains all the one and two letter level codes and explanations as to why each letter was chosen. Unfortunately, it was not possible to come up with French equivalents to all the letter level codes. Therefore, to maintain commonality and to minimize confusion, the French and English codes are identical.

Criteria	Letter Codes	Full Rating Title	Range
Confidentiality	**CC**	**C**overt Channels	CC-0 – CC-3
	CD	**D**iscretionary Confidentiality	CD-0 – CD-4
	CM	**M**andatory Confidentiality	CM-0 – CM-4
	CR	Object **R**euse	CR-0 – CR-1
Integrity	**ID**	**D**iscretionary Integrity	ID-0 – ID-4
	IM	**M**andatory Integrity	IM-0 – IM-4
	IP	**P**hysical Integrity	IP-0 – IP-4
	IR	**R**ollback	IR-0 – IR-2
	IS	**S**eparation of Duties	IS-0 – IS-3
	IT	Self **T**esting	IT-0 – IT-3
Availability	**AC**	**C**ontainment	AC-0 – AC-3
	AF	**F**ault Tolerance	AF-0 – AF-2

Table 2 Criteria Letter Codes. (Continued . . .)

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

	AR	**R**obustness	AR-0	–	AR-3
	AY	Recover**y**	AY-0	–	AY-3
Accountability (Who)	**WA**	**A**udit	WA-0	–	WA-5
	WI	**I**dentification and Authentication	WI-0	–	WI-3
	WT	**T**rusted Path	WT-0	–	WT-2
Assurance (Trust)	**T**	Levels of Assurance	T-0	–	T-7

Table 2 Criteria Letter Codes.

An example of a rating would be CD-2, CR-1, AC-1, WI-1, WA-2, T-2.

Constraints

In some cases, a specific service is not valid without other services. Whenever this is the case, a constraint indicates the other required services and their corresponding levels. To ensure visibility, the following format is used:

CONSTRAINT: CR-1.

The constraints listed are the ones directly required for the given service to perform properly. The constraint list is a *minimal* list, therefore, the services listed may also be constrained by another service which may not be directly required. For the full set of constraints for a given level of service see Appendix B.

Appendices

Informative appendices are provided to aid in the understanding of the Criteria. These appendices include discussions of various security policy models and their applicability to the Criteria, guidelines to the five criteria, and explanations of the ideas and rationale behind the Criteria.

Each appendix uses the Criteria as a base of reference and stands on its own. The only cross references within the appendices are to Criteria itself.

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

Fundamentals

The Criteria is based on three elements: mediation, isolation, and audit. From these three elements four basic "policies" can be developed: confidentiality, the ability to prevent release of information to unauthorized individuals; integrity, the ability to prevent modification by unauthorized individuals; availability, the ability to indicate, with some level of precision, the ability of a product to withstand a denial of service attack or failure; and accountability, the ability to hold people responsible for their actions. A further requirement is necessary to ensure that the four basic "policies" are complete and cohesive, that element is assurance. Assurance provides an all encompassing level of trust to which the various "policies" within the product can be evaluated.

A further discussion of these fundamentals, and the method by which the various services can be defined through them, is provided in Appendices C and D.

Products vs. Systems

The Canadian Criteria is a product oriented criteria. Products are broadly defined as any grouping of software, hardware, and/or firmware provided by a vendor, or vendors acting in a consortium, which provide a uniform security policy and uniform look and feel. Two types of systems exist: non-homogenous (or heterogenous) and homogenous.

Non-homogenous systems are defined as groups of products without a uniform security policy, and are not covered by these criteria. The study of computer security in non-homogenous systems remains an open research topic.

Any product which consists of more than one component, such as a network, is known as a homogenous system *if it abides by the product restrictions above.* This definition allows for the inclusion of networks, distributed systems, etc, within the context of the Canadian Criteria *without* the requirement for additional interpretations.

Trusted Computing Bases

A Trusted Computing Base (TCB) is the set of elements of a product, including any hardware, firmware and software, involved in enforcing a product's security policy; or those elements involved in enforcing a given service policy when used in relation to a specific service. The TCB does not, and most probably **is not**, the entire product but rather a specific portion thereof. Any aspect of a product which, if manipulated by an outside entity, would violate the security policy of the product must be considered as part of the TCB.

Those aspects which are considered part of the TCB are defined to be within the TCB boundary. The boundary must be defined as the scope of control to which the TCB maintains enforcement of the product's security policy. The boundary should include all entities which manipulate or are manipulated by the TCB and that require protection form outside interference.

Security Policy

There must be an explicit security policy enforced by the product. The security policy is the set of rules regulating the use of information, including its processing, storage, distribution and presentation in a product. The security policy must be specified in the manner defined within the targeted assurance level.

Isolation, Mediation, & Audit

The purpose of a trusted product is to isolate objects within its control, to guarantee the mediation of access requests, and to insure a controlled and noncircumventable audit exists to track information flow within the trusted product. All security functionality falls within the bounds of one or more of isolation, mediation, or audit.

Objects

In the Canadian Criteria everything under the control of the TCB can be termed an object. Objects can be in one of three states (see Figure 5): user, process, or passive. Entering a given state simply means that the object is viewed by the TCB in a different context. However, an object (be it a user, process or passive object) can be manipulated as an object by other processes.

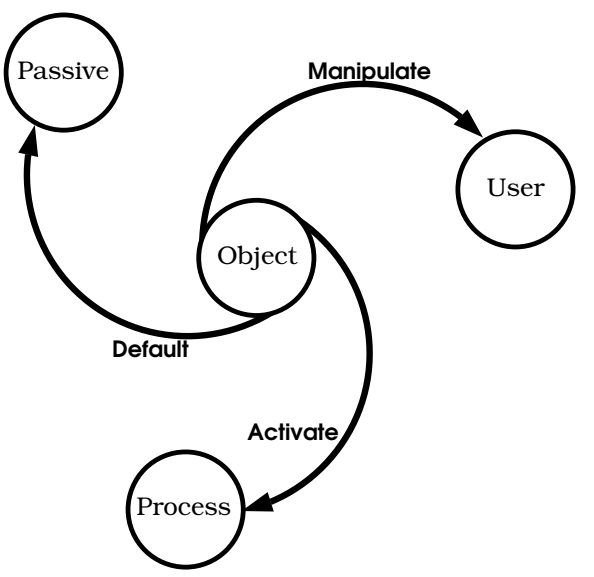


Figure 5: State Transitions from an Entity to an Object, User, or Process

The user state is entered by an object whenever an individual logs into the product. The entity in question is the TCB's image of the user. This is, usually, followed by invocation (or activation) of a process on that user's behalf. This process is the true manipulator of the objects within the user's domain. Because all entities within a product can be manipulated, and by default are in the passive state, the Criteria sometimes refers to all entities as *objects.* User objects and process objects are referred to solely as *user* and *process*, respectively.

The flow of information between the three types of objects is shown in Figure 6 and expanded upon in Appendices E, F, and G.

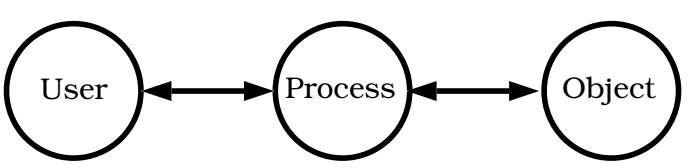


Figure 6: Information Flow Between User, Process, and Object

Object Space The object space of a TCB, illustrated in Figures 7 and 8, contains all the objects under the control of the reference monitor. As users log into the product, they are instantiated into a *user object* within the product. Each user object, *user* for short, is an object from the viewpoint of the TCB. As users initiate processes, the processes are (possibly) associated with the invoking user. Processes, as do users, remain objects and can be so manipulated within the limits of the security policy.

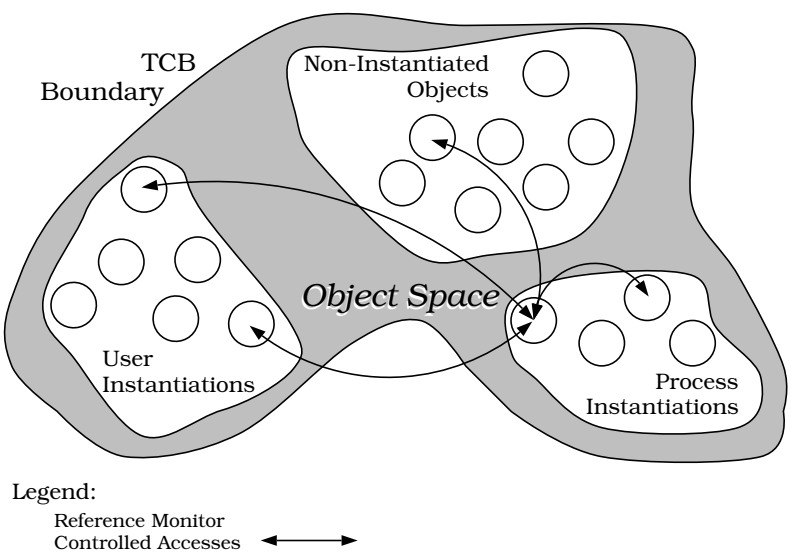


Figure 7: Interaction Between TCB Controlled Objects

For illustration purposes, Figure 7 presents an active object space. The illustration shows two users using a single process, which in turn is manipulating another process as well as a "non-instantiated object"[8]. But, the figure could be

[8] A *non-instantiated object* is simply any other object in the system which has not entered either the user or process states.

interpreted as the process manipulating other objects in the object space, objects which include the two user objects, the passive object and the other process object.

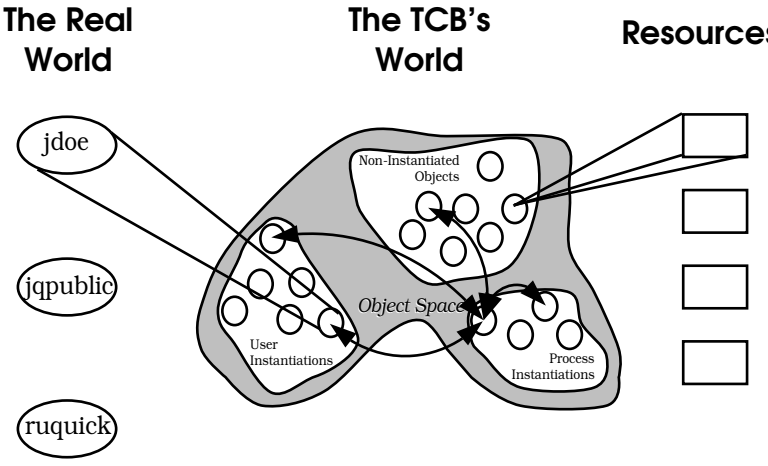


Figure 8: Objects and Their Counterparts

Figure 8 presents the entire picture. Any given object can be an encapsulator for protected resources. User objects are instantiations within the product of actual users in the real world[9]. And, process objects are those objects which the product is actually executing in some way. Whenever a user logs off or a process terminates execution, they revert to passive objects in the non-instantiated group. The destruction and creation of objects is defined by the vendor and must not contravene any aspects of the security policy. All creation, destruction, and instantiation must be performed by the trusted computing base. All mediation must be performed by the reference monitor[10].

The objects in a product are defined by the vendor and approved by CSE. Objects within a product can range from files to devices to ports to printers. Anything protected under the security policy must be defined as an object. All objects must have unique identifying tags which are to be used by the TCB for isolation,

[9] These real users can actually be daemons or ghosts, used for autonomous processing.

[10] If a reference monitor is not used, the vendor must provide sufficient evidence that the chosen method of mediation is capable of enforcing the security policy. The evaluation authority requires a strong, noncircumventable mechanism capable of providing the mediation services.

mediation, and audit. Objects *not* protected by the TCB exist outside the TCB boundary are accessible, but are not illustrated in Figures 7 or 8.

Tagged Objects The set of rules (in a product) governing the interaction between objects is known as the security policy. Each object is tagged with a unique identifier and with further information denoting its access rights and privileges. Tag is a term used to describe any access mediation information associated with users, processes, or objects. The association of a tag with an entity may be explicit or implicit. The tag of an entity is part of its encapsulation by the TCB.

The number of tags and identifiers associated with an object can be unlimited. As users and processes attempt to access objects, the mediation services[11] can make decisions based on the security policy, by examining the tags, as to the validity of the access requests.

With the tags and a security policy, one can design discretionary controls, mandatory controls, integrity controls, and a wide variety of other controls over objects.

TCSEC Subjects in the Canadian Criteria The US TCSEC uses the term "subjects" to define active objects within a trusted product. In the Canadian Criteria "subjects" are defined as *users*, the object invoking the actions, and *processes*, the object acting on behalf of the user to perform the actions.

To a process, everything within the product is an "object". A user, for example, is an object that the process reads from and writes to. All processes are owned, have a specific user as initiator, and are controlled by this owner.

This splitting of the TCSEC's "subject" into "process" and "user" aids in describing exact interactions within the product, especially when describing policy issues at the higher levels of assurance or enhanced accountability and access controls. This division allows for restricted access to passive objects by specific processes, a fundamental requirement of integrity. Modification of an object requires: i) access to the process; and ii) access by the process **and** the user to passive object.

[11] One valid implementation of mediation services is a reference monitor (see Appendices C and D.

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

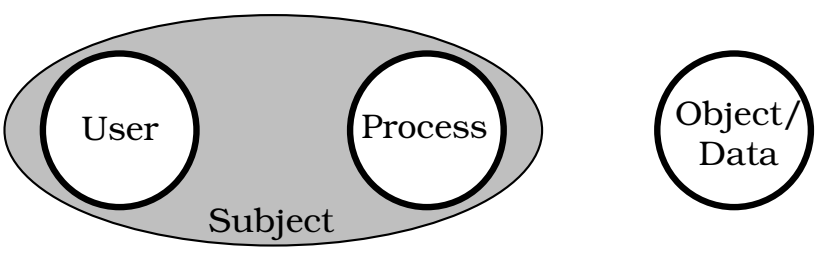


Figure 9: "Objects" in the TCSEC and the Canadian Criteria

Figure 9 shows the mapping of the TCSEC definition of a subject to that of the Canadian Criteria's user and process. Objects which are to be manipulated are known as objects in both the TCSEC and Canadian Criteria.

Continuous Protection

The services that enforce the security policy must be continuously protected against tampering and/or unauthorized changes. No computer product can be considered truly secure if the basic software, hardware and firmware mechanisms that enforce the security policy are themselves subject to unauthorized modification or subversion.

Security Services & Mechanisms

A service is a generic term to define some form of security functionality that is offered by a product. Each service can be implemented by one or more underlying mechanisms, where the mechanisms are product dependent. In other words, a service is an abstraction while the security mechanisms are the implementation of that service within a given product. A given set of security mechanisms *can* implement more than one service. For example, it is feasible for a vendor to implement both Mandatory, under control of the system, and Discretionary, under control of individual users, Confidentiality services with a single set of mechanisms, resulting in ratings for both types of service.

The Canadian Criteria list a set of services. The set, although well defined, is not exhaustive. Solutions to security problems not yet envisioned may not be covered by the listed services.

Inclusion of New Services

The Canadian Criteria and the associated services described herein are not meant to be a final answer to the problems of computer security. Rather, the Canadian Criteria offer a set of well understood services which can be used to create trusted products which can reflect the requirements of the market.

The document does not assume to include all possible services that can be foreseen but rather contains those which are known to be *good* services at time of release. If a given Vendor can show, to the evaluating authority's satisfaction, that a new or modified form of service provides sufficient protection against a specific type of threat or offers functionality not currently provided in any other

form within the Criteria, then CSE will examine the strength and usefulness of such a service. CSE will indicate to the Vendor whether such a service is appropriate and how the evaluation of the service will be carried out relative to the Criteria.

If the service does prove to be generally useful or a general improvement in functionality, then the Criteria Working Group will consider its inclusion in the next revision of the Criteria.

Modularity

In defining modularity, one could envision those aspects of the product which are coded within specific "structured programming" conventions. However, the Canadian Criteria reference to modularity is in terms of the overall design of the product. The coding or implementation practices (such as structured programming) are assurance issues and are discussed in the Assurance Criteria as well as in Appendix J.

For a TCB to be termed modular it would have to be designed into logical groupings of software, hardware, and/or firmware with each grouping performing predefined tasks. The strictness of this definition is dependent upon the level of assurance the Vendor is attempting to attain. At the lower levels of assurance, modularity can be defined in terms of grouping similar functionality into given source files. At the higher levels, data hiding, encapsulation, and other techniques would be used to ensure that each module performs a single task and that all manipulated objects are either locally defined and accessed or passed via parameters or similar technique.

The overall product, which could comprise networks and distributed systems as well as databases, must be modular in the sense that any inter-process communication is only accomplished via known and described channels.

Composable Evaluations

With the nature of current products tending towards heavily distributed architectures, efforts have begun to work out a method of evaluation based on composable products. As research continues, composable evaluations of properly defined composable products will enter the mainstream from the research arena. Composable products and evaluations would allow Vendors to modify existing trusted products and retain or improve their ratings without having the *entire* product reevaluated.

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

Confidentiality Criteria

A product which is rated against the Confidentiality Criteria must provide services capable of protecting resources against unauthorized disclosure. Confidentiality may be provided in a product through a *covert channel analysis*, and through the use of *discretionary confidentiality* services, *mandatory confidentiality* services, and *object reuse* services.

Covert Channels

A covert channel analysis is performed in order to identify those information flows which exist in a product but cannot be controlled through other services. The Covert Channel levels of service rate the services based upon the analysis performed, and on the ability to audit and eliminate covert channels.

A general guide to covert channel analysis is found in Appendix F.

CC–0
Non-compliant

This level is reserved for those products which have been evaluated under the Covert Channel Service and have failed to meet the requirements of a higher level of service.

CC–1
Covert Channel Analysis

A covert channel analysis shall be conducted. Each identified hardware, firmware and software covert channel shall be documented.

The maximum bandwidth (determined by actual measurement or by engineering estimation) of each identified covert channel shall be documented.

Identified covert channels which can be used in aggregate shall have their aggregate bandwidth documented.

CONSTRAINT: CR-1, T-3

CC–2
Auditable Covert Channels

A covert channel analysis shall be conducted. Each identified hardware, firmware and software covert channel shall be documented.

The maximum bandwidth (determined by actual measurement or by engineering estimation) of each identified covert channel shall be documented.

Identified covert channels which can be used in aggregate shall have their aggregate bandwidth documented.

The TCB shall be able to audit an approved subset of the identified covert channels.

CC–3
Elimination of Covert Channels

Confidentiality Criteria

CONSTRAINT: CR-1, **WA-1**, T-3

A covert channel analysis shall be conducted. Each identified hardware, firmware and software covert channel shall be documented.

Each identified covert channel shall be eliminated from the product.

CONSTRAINT: CR-1, T-3

Discretionary Confidentiality

Discretionary confidentiality services allow authorized users to control the flow of information within from protected objects to users a product. The Discretionary Confidentiality levels of service rate these services based on the strength of the mechanism and their granularity of control.

Appendix E and Appendix F provide guidance on meeting the discretionary confidentiality criteria.

CD–0
Non-compliant

This level is reserved for those products which have been evaluated under the Discretionary Confidentiality service and have failed to meet the requirements of a higher level of service.

CD–1
Minimal Discretionary Confidentiality

The TCB shall enforce an approved discretionary confidentiality policy to protect against information disclosure. The approved policy shall define the set of the product's objects to which it applies.

Access mediation by the TCB shall be based upon the tag of the process and the tag of the protected object.

Requests for changes to access mediation information shall be serviced by the TCB based upon the user tag of the requesting user or process.

Access mediation information shall be associated with each protected object upon creation or initialization.

Rules for preserving the tags of protected objects during their export/import shall be provided as part of the discretionary confidentiality policy.

CONSTRAINT: CR-1, WI-1

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

Discretionary Confidentiality

CD–2
Basic Discretionary Confidentiality

The TCB shall enforce an approved discretionary confidentiality policy to protect against information disclosure. The approved policy shall define the set of the product's objects to which it applies.

Access mediation by the TCB shall be based upon the tag **of the user** and the tag of the protected object.

The discretionary confidentiality policy shall provide a partial representation of the access matrix of all user tags and protected object tags.

Requests for changes to access mediation information shall be serviced by the TCB based upon the user tag of the requesting user or process.

Access mediation information shall be associated with each protected object upon creation or initialization.

Rules for preserving the tags of protected objects during their export/import shall be provided as part of the discretionary confidentiality policy.

CONSTRAINT: CR-1, WI-1

CD–3
Controlled Discretionary Confidentiality

The TCB shall enforce an approved discretionary confidentiality policy to protect against information disclosure. The approved policy shall define the set of the product's objects to which it applies.

Access mediation by the TCB shall be based upon the tag of the user and the tag of the protected object.

The discretionary confidentiality policy shall provide a **full** representation of the access matrix of all user tags and protected object tags.

Requests for changes to access mediation information shall be serviced by the TCB based upon the user tag of the requesting user or process.

Access mediation information shall be associated with each protected object upon creation or initialization.

Rules for preserving the tags of protected objects during their export/import shall be provided as part of the discretionary confidentiality policy.

CONSTRAINT: CR-1, WI-1

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

CD–4
Advanced Discretionary Confidentiality

The TCB shall enforce an approved discretionary confidentiality policy to protect against information disclosure. The approved policy shall define the set of the product's objects to which it applies.

Access mediation by the TCB shall be based upon the tag of the user, **the tag of the process** and the tag of the protected object.

The discretionary confidentiality policy shall provide a full representation of the access matrix of all user tags, **process tags** and protected object tags.

Requests for changes to access mediation information shall be serviced by the TCB based upon the user tag of the requesting user or process.

Access mediation information shall be associated with each protected object upon creation or initialization.

Rules for preserving the tags of protected objects during their export/import shall be provided as part of the discretionary confidentiality policy.

CONSTRAINT: CR-1, WI-1

Mandatory Confidentiality

Mandatory confidentiality services allow an authorized administrator or user to control the flow of information from protected objects to users within a product. The Mandatory Confidentiality levels of service rate these services based on the extent and strength of control.

A general guide to mandatory confidentiality is found in Appendix E and Appendix F.

CM–0
Non-compliant

This level is reserved for those products which have been evaluated under the Mandatory Confidentiality service and have failed to meet the requirements of a higher level of service.

CM–1
Minimal Mandatory Confidentiality

The TCB shall enforce an approved mandatory confidentiality policy to protect against information disclosure. The approved policy shall define the set of the product's objects to which it applies.

Access mediation by the TCB shall be based upon the tag of the process and the tag of the protected object.

Requests for changes to access mediation information shall only be serviced by the TCB for administrators and users to whom the required authority has been delegated.

Access mediation information shall be associated with each protected object upon creation or initialization.

Rules for preserving the tags of protected objects during their export/import shall be provided as part of the mandatory confidentiality policy.

CONSTRAINT: CR-1, IS-1

CM–2
Basic Mandatory Confidentiality

The TCB shall enforce an approved mandatory confidentiality policy to protect against information disclosure. The approved policy shall define the set of the product's objects to which it applies.

Access mediation by the TCB shall be based upon the tag **of the user** and the tag of the protected object.

Requests for changes to access mediation information shall only be serviced by the TCB for administrators and users to whom the required authority has been delegated.

Access mediation information shall be associated with each protected object upon creation or initialization.

Rules for preserving the tags of protected objects during their export/import shall be provided as part of the mandatory confidentiality policy.

CONSTRAINT: CR-1, IS-1, WI-1

CM–3
Controlled Mandatory Confidentiality

The TCB shall enforce an approved mandatory confidentiality policy to protect against information disclosure. The approved policy shall apply to **all of the product's objects**.

Access mediation by the TCB shall be based upon the tag of the user and the tag of the protected object.

Requests for changes to access mediation information shall only be serviced by the TCB for administrators and users to whom the required authority has been delegated.

Access mediation information shall be associated with each protected object upon creation or initialization.

Rules for preserving the tags of protected objects during their export/import shall be provided as part of the mandatory confidentiality policy.

CONSTRAINT: CR-1, IS-1, WI-1

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

DRAFT

Confidentiality Criteria

CM–4
Advanced Mandatory Confidentiality

The TCB shall enforce an approved mandatory confidentiality policy to protect against information disclosure. The approved policy shall apply to all of product's objects.

Access mediation by the TCB shall be based upon the tag of the user, **the tag of the process** and the tag of the protected object.

Requests for changes to access mediation information shall only be serviced by the TCB for administrators and users to whom the required authority has been delegated.

Access mediation information shall be associated with each protected object upon creation or initialization.

Rules for preserving the tags of protected objects during their export/import shall be provided as part of the mandatory confidentiality policy.

CONSTRAINT: CR-1, IS-1, WI-1

Object Reuse

The Object Reuse service provides for the proper reuse of shared storage objects. Object reuse involves ensuring that when a shared object is reassigned or reallocated to a user or process that no information remains in the shared object from a previous user or process.

CR–0
Non-compliant

This level is reserved for those products which have been evaluated under the Object Reuse service and have failed to meet the requirements of a higher level of service.

CR–1
Object Reuse

The TCB shall enforce an approved object reuse policy. The approved policy shall apply to all of product's shared objects.

All previous authorization and access to a protected object shall be revoked prior to reassignment or reallocation.

All previous information content of a protected object shall be made unavailable prior to reassignment or reallocation.

CONSTRAINT: None.

Integrity Criteria

A product which is rated against the Integrity Criteria must provide services capable of providing information integrity or product integrity. Integrity may be provided in a product through the use of *discretionary integrity* services, *mandatory integrity* services, *physical integrity* services, *rollback* services, *self test* services and *separation of duties* services.

Discretionary Integrity

Discretionary integrity services allow authorized users to control the flow of information from users to protected objects within a product. The Discretionary Integrity levels of service rate these services based on the strength of the mechanism and the granularity of control.

Appendix E and Appendix G provide guidance on meeting the discretionary integrity criteria.

ID–0
Non-compliant

This level is reserved for those products which have been evaluated under the Discretionary Integrity service and have failed to meet the requirements of a higher level of service.

ID–1
Minimal Discretionary Integrity

The TCB shall enforce an approved discretionary integrity policy to protect against information modification. The approved policy shall define the set of the product's objects to which it applies.

Access mediation by the TCB shall be based upon the tag of the user and the tag of the protected object.

Requests for changes to access mediation information shall be serviced by the TCB based upon the user tag of the requesting user or process.

Access mediation information shall be associated with each protected object upon creation or initialization.

Rules for preserving the tags of protected objects during their export/import shall be provided as part of the discretionary integrity policy.

CONSTRAINT: CR-1, WI-1

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

DRAFT

ID–2
Basic Discretionary Integrity

The TCB shall enforce an approved discretionary integrity policy to protect against information modification. The approved policy shall define the set of the product's objects to which it applies.

Access mediation by the TCB shall be based upon the tag **of the process** and the tag of the protected object.

The discretionary integrity policy shall provide a partial representation of the access matrix of all process tags and protected object tags.

Requests for changes to access mediation information shall be serviced by the TCB based upon the user tag of the requesting user or process.

Access mediation information shall be associated with each protected object upon creation or initialization.

Rules for preserving the tags of protected objects during their export/import shall be provided as part of the discretionary integrity policy.

CONSTRAINT: CR-1, WI-1

ID–3
Controlled Discretionary Integrity

The TCB shall enforce an approved discretionary integrity policy to protect against information modification. The approved policy shall define the set of the product's objects to which it applies.

Access mediation by the TCB shall be based upon the tag of the process and the tag of the protected object.

The discretionary integrity policy shall provide a **full** representation of the access matrix of all process tags and protected object tags.

Requests for changes to access mediation information shall be serviced by the TCB based upon the user tag of the requesting user or process.

Access mediation information shall be associated with each protected object upon creation or initialization.

Rules for preserving the tags of protected objects during their export/import shall be provided as part of the discretionary integrity policy.

CONSTRAINT: CR-1, WI-1

ID–4
Advanced Discretionary Integrity

The TCB shall enforce an approved discretionary integrity policy to protect against information modification. The approved policy shall define the set of the product's objects to which it applies.

Access mediation by the TCB shall be based upon the tag of the process, **the tag of the user** and the tag of the protected object.

The discretionary integrity policy shall provide a full representation of the access matrix of all user tags, **process tags** and protected object tags.

Requests for changes to access mediation information shall be serviced by the TCB based upon the user tag of the requesting user or process.

Access mediation information shall be associated with each protected object upon creation or initialization.

Rules for preserving the tags of protected objects during their export/import shall be provided as part of the discretionary integrity policy.

CONSTRAINT: CR-1, WI-1

Mandatory Integrity

Mandatory integrity services allow an administrator or authorized user to control the flow of information from users to protected objects within a product. The Mandatory Integrity levels of service rate these services based on the extent and strength of control over product objects.

A general guide to mandatory integrity is found in Appendix E and Appendix G.

IM–0
Non-compliant

This level is reserved for those products which have been evaluated under the Mandatory Integrity service and have failed to meet the requirements of a higher level of service.

IM–1
Minimal Mandatory Integrity

The TCB shall enforce an approved mandatory integrity policy to protect against information modification. The approved policy shall define the set of the product's objects to which it applies.

Access mediation by the TCB shall be based upon the tag of the user and the tag of the protected object.

Requests for changes to access mediation information shall only be serviced by the TCB for administrators and users to whom the required authority has been delegated.

Access mediation information shall be associated with each protected object upon creation or initialization.

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

Integrity Criteria

IM–2
Basic Mandatory Integrity

Rules for preserving the tags of protected objects during their export/import shall be provided as part of the mandatory integrity policy.

CONSTRAINT: CR-1, IS-1, WI-1

The TCB shall enforce an approved mandatory integrity policy to protect against information modification. The approved policy shall define the set of the product's objects to which it applies.

Access mediation by the TCB shall be based upon the tag **of the process** and the tag of the protected object.

Requests for changes to access mediation information shall only be serviced by the TCB for administrators and users to whom the required authority has been delegated.

Access mediation information shall be associated with each protected object upon creation or initialization.

Rules for preserving the tags of protected objects during their export/import shall be provided as part of the mandatory integrity policy.

CONSTRAINT: CR-1, IS-1

IM–3
Complete Mandatory Integrity

The TCB shall enforce an approved mandatory integrity policy to protect against information modification. The approved policy shall apply to **all of the product's objects**.

Access mediation by the TCB shall be based upon the tag of the process and the tag of the protected object.

Requests for changes to access mediation information shall only be serviced by the TCB for administrators and users to whom the required authority has been delegated.

Access mediation information shall be associated with each protected object upon creation or initialization.

Rules for preserving the tags of protected objects during their export/import shall be provided as part of the mandatory integrity policy.

CONSTRAINT: CR-1, IS-1

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

IM–4
Advanced Mandatory Integrity

The TCB shall enforce an approved mandatory integrity policy to protect against information modification. The approved policy shall apply to all of product's objects.

Access mediation by the TCB shall be based upon the tag of the process, **the tag of the user** and the tag of the protected object.

Requests for changes to access mediation information shall only be serviced by the TCB for administrators and users to whom the required authority has been delegated.

Access mediation information shall be associated with each protected object upon creation or initialization.

Rules for preserving the tags of protected objects during their export/import shall be provided as part of the mandatory integrity policy.

CONSTRAINT: CR-1, IS-1

Physical Integrity

Physical integrity defines the physical perimeter of the TCB and provides services for the physical protection of the components within that boundary. These services are used to indicate or restrict unauthorized physical access to the internals of the product and to deter unauthorized use, modification or substitution of the protected components. The Physical Integrity levels of service rate these services based on the type of protection provided, and the degree of effort required to defeat it.

IP–0
Non-compliant

This level is reserved for those products which have been evaluated under the Physical Integrity service and have failed to meet the requirements of a higher level of service.

IP–1
Basic Physical Integrity

The TCB shall enforce an approved physical integrity policy. The policy shall include a description of the physical perimeter of the TCB and shall define the set of the product's components to which it applies.

The physical perimeter shall be protected by tamper evident mechanisms such that unauthorized use of, physical access to, or physical modification of the protected components will be detected after the unauthorized attempt.

CONSTRAINT: None.

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

Integrity Criteria

IP–2
Intermediate Physical Integrity

The TCB shall enforce an approved physical integrity policy. The policy shall include a description of the physical perimeter of the TCB and shall define the set of the product's components to which it applies.

The physical perimeter shall be protected by tamper **resistant** mechanisms such that unauthorized use of, physical access to, or physical modification of the protected components will be **unsuccessful**.

Covers and openings through the physical perimeter shall be protected by tamper response mechanisms such that unauthorized use of, physical access to, or physical modification of the protected components will be detected during the unauthorized attempt.

CONSTRAINT: None.

IP–3
Advanced Physical Integrity

The TCB shall enforce an approved physical integrity policy. The policy shall include a description of the physical perimeter of the TCB and shall define the set of the product's components to which it applies.

The physical perimeter shall be protected by tamper resistant mechanisms such that unauthorized use of, physical access to, or physical modification of the protected components will be unsuccessful.

Covers and openings through the physical perimeter shall be protected by tamper response mechanisms such that unauthorized use of, physical access to, or physical modification of the protected components will be detected during the unauthorized attempt.

All components within the physical perimeter shall be protected against failure due to extreme environmental conditions.

CONSTRAINT: None.

IP–4
Complete Physical Integrity

The TCB shall enforce an approved physical integrity policy. The policy shall include a description of the physical perimeter of the TCB and shall define the set of the product's components to which it applies.

All components within the physical perimeter shall be protected by tamper resistant mechanisms such that unauthorized use of, physical access to, or physical modification of the protected components will be unsuccessful.

All components within the physical perimeter shall be protected by tamper response mechanisms such that unauthorized use of, physical access to, or physical modification of the protected components will be detected during the unauthorized attempt.

All components within the physical perimeter shall be protected against failure due to extreme environmental conditions.

CONSTRAINT: None.

Rollback

Rollback services provide the ability to undo an action or a series of actions and return a protected object to a previous state. The Rollback levels of service rate these services based on the granularity of objects and operations which can be rolled back.

IR–0
Non-compliant

This level is reserved for those products which have been evaluated under the Rollback service and have failed to meet the requirements of a higher level of service.

IR–1
Restricted Rollback

The TCB shall enforce an approved rollback policy. The approved policy shall define the set of the product's objects to which it applies.

The policy shall provide an automated means to allow authorized users or processes to rollback, or undo, a defined set of operations on protected objects over a predefined period of time.

CONSTRAINT: WI-1

IR–2
Advanced Rollback

The TCB shall enforce an approved rollback policy. The approved policy shall define the set of the product's objects to which it applies.

The policy shall an automated means to allow authorized users or processes to rollback, or undo, **all** operations on protected objects over a predefined period of time.

CONSTRAINT: WI-1

DRAFT DRAFT DRAFT DRAFT DRAFT

Separation of Duties

Separation of duties services provide for the compartmentalization of responsibility and reduces the potential damage from a corrupt user or administrator and places limits on the authority of the user or administrator. The Separation of Duties levels of service rate these services based on the granularity of separation between users and administrative responsibilities.

IS–0
Non-compliant

This level is reserved for those products which have been evaluated under the Separation of Duties service and have failed to meet the requirements of a higher level of service.

IS–1
Basic Separation of Duties

The TCB shall enforce an approved separation of duties policy. The policy shall identify administrative and nonadministrative user roles and their respective functions.

The policy shall define an explicit user action required to be performed before a user can assume a role that they are authorized for.

CONSTRAINT: WI-1

IS–2
Administrative Separation of Duties

The TCB shall enforce an approved separation of duties policy. The policy shall identify administrative and nonadministrative user roles and their respective functions.

The policy shall define an explicit user action required to be performed before a user can assume a role that they are authorized for.

The policy shall define at least two distinct administrative roles: a security administrator and non-security administrator.

The functions assigned to each administrative role shall be minimized to include only those functions required for the performance of that role.

CONSTRAINT: WI-1

IS–3
Privilege-based Separation of Duties

The TCB shall enforce an approved separation of duties policy. The policy shall identify administrative and nonadministrative user roles and their respective functions.

The policy shall define an explicit user action required to be performed before a user can assume a role that they are authorized for.

The policy shall define at least two distinct administrative roles: a security administrator and non-security administrator.

The functions assigned to each administrative role shall be minimized to include only those functions required for the performance of that role.

The policy shall define multiple distinct user roles.

CONSTRAINT: WI-1

Self Testing

Self testing services allow the TCB to ensure correct operation and integrity for defined product functions. The Self Testing levels of service rate these services based on the ability of the mechanism to provide timely reports of incorrectly functioning product components.

IT–0
Non-compliant

This level is reserved for those products which have been evaluated under the Self Testing service and have failed to meet the requirements of a higher level of service.

IT–1
Basic Self Testing

The TCB shall enforce an approved self testing policy. The policy shall describe the product features that can be used to periodically validate the correct operation of the TCB.

The coverage and use of the tests shall be described in the Trusted Facility Manual.

CONSTRAINT: None.

IT–2
Intermediate Self Testing

The TCB shall enforce an approved self testing policy. The policy shall describe the product features that can be used to periodically validate the correct operation of the TCB.

The TCB shall run a suite of self tests during initial start-up in order to validate the correct operation of its critical functions.

The coverage and use of the tests shall be described in the Trusted Facility Manual.

CONSTRAINT: None.

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

IT–3
Advanced Self Testing

Integrity Criteria

The TCB shall enforce an approved self testing policy. The policy shall describe the product features that can be used to periodically validate the correct operation of the TCB.

The TCB shall run a suite of self tests during initial start-up **and during normal product operation** in order to validate the correct operation of its critical functions.

The coverage and use of the tests shall be described in the Trusted Facility Manual.

CONSTRAINT: None.

Availability Criteria

A product which is rated against the Availability Criteria must provide services capable of controlling the availability of a product. Availability may be provided in a product through the use of *containment* services, *fault tolerance* services, *robustness* services, and *recovery* services.

Containment

Containment services allow the TCB to control the use of services and resources by users. The Containment levels of service are based upon the extent and strength of control exerted over the availability of the product services.

AC–0
Non-compliant

This level is reserved for those products which have been evaluated under the Containment service and have failed to meet the requirements of a higher level of service.

AC–1
Quotas

The TCB shall enforce an approved containment policy. The policy shall define the set of the product's objects and the capability to place limits on the allocation to users of these objects.

Requests for changes to assigned limits shall only be serviced by the TCB for administrators and users to whom the required authority has been delegated.

CONSTRAINT: IS-1

AC–2
Denial of Service

The TCB shall enforce an approved containment policy. The policy shall define the capability to place limits on the allocation to users of **all of the product's** objects.

Requests for changes to assigned limits shall only be serviced by the TCB for administrators and users to whom the required authority has been delegated.

Limits shall be able to be set such that the TCB can prevent any single user from being able to deny other users access to TCB functions or protected objects.

CONSTRAINT: IS-1

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

Availability Criteria

AC–3
Resource Restrictions

The TCB shall enforce an approved containment policy. The policy shall define the capability to place limits on the allocation to users **and to configurable groups of users** of all of the product's objects.

Requests for changes to assigned limits shall only be serviced by the TCB for administrators and users to whom the required authority has been delegated.

Limits shall be able to be set such that the TCB can prevent any single user **or configurable group of users** from being able to deny other users access to TCB functions or protected objects.

CONSTRAINT: IS-1

Fault Tolerance

Fault Tolerance services allow the TCB to ensure availability of the product after component failures. The Fault Tolerance levels of service rate these services based on the ability to have components replaced without discontinuing serivce.

AF–0
Non-compliant

This level is reserved for those products which have been evaluated under the Fault Tolerance service and have failed to meet the requirements of a higher level of service.

AF–1
Limited Hot Replacement

The vendor shall conduct a component failure analysis study for the product.

The TCB shall enforce an approved fault tolerance policy. The policy shall define the set of the product's components which can be replaced without incurring a service discontinuity.

An administrator, or users to whom the required authority has been delegated, shall be able to replace any protected component.

CONSTRAINT: IS-1, AR-1

AF–2
Hot Replacement

The vendor shall conduct a component failure analysis study for the product.

The TCB shall enforce an approved fault tolerance policy. The policy shall **apply to all of the product's components and shall allow their replacement** without incurring a service discontinuity.

An administrator, or users to whom the required authority has been delegated, shall be able to replace any protected component.

CONSTRAINT: IS-1, AR-1

Robustness

Robustness services allow the TCB to ensure availability of the product after component failures. The Robustness levels of service rate these services based on the ability of the TCB to continue operating based upon the number of failures and the service available after a failure.

AR–0
Non-compliant

This level is reserved for those products which have been evaluated under the Robustness service and have failed to meet the requirements of a higher level of service.

AR–1
Reliability under Limited Failure

The vendor shall conduct a component failure analysis study for the product.

The TCB shall enforce an approved robustness policy. The policy shall define the set of the product's components and those components' modes of failure after which the product can continue operation.

Failure of any single protected component shall not result in loss of all service but instead result in, at worst, a degraded mode of operation.

Thresholds at which failures will result in degraded service or loss of service shall be clearly identified.

The product shall be capable of notifying an administrator of the failure of any protected component.

CONSTRAINT: IS-1

AR–2
Reliability with Degraded Service

The vendor shall conduct a component failure analysis study for the product.

The TCB shall enforce an approved robustness policy. The policy shall **apply to all of the product's components.**

Failure of any single protected component shall not result in loss of all service but instead result in, at worst, a degraded mode of operation.

Thresholds at which failures will result in degraded service or loss of service shall be clearly identified.

The product shall be capable of notifying an administrator of the failure of any protected component.

CONSTRAINT: IS-1

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

AR–3
Reliability with Full Service

The vendor shall conduct a component failure analysis study for the product.

The TCB shall enforce an approved robustness policy. The policy shall apply to all of the product's components.

Failure of any single protected component **shall not result in a loss of service or service degradation.**

Thresholds at which failures will result in degraded service or loss of service shall be clearly identified.

The product shall be capable of notifying an administrator of the failure of any protected component.

CONSTRAINT: IS-1

Recovery

Recovery services allow the TCB to return to a known trusted state after a product failure or service discontinuity. The Recovery levels of service rate these services based on the degree of automation associated with the trusted recovery.

AY–0
Non-compliant

This level is reserved for those products which have been evaluated under the Recovery service and have failed to meet the requirements of a higher level of service.

AY–1
Manual Recovery

The TCB shall enforce an approved recovery policy. The policy shall define the product failures and service discontinuities from which recovery is possible in a trusted manner.

After a product failures or service discontinuity, the TCB shall enter a state where only administrators, and users to whom the required authority has been delegated, are capable of returning the product to normal operation.

Manual procedures shall be provided by which the product can be returned to normal operation in a trusted manner.

Thresholds at which discontinuities require that the product be re-installed shall be identified.

CONSTRAINT: IS-1

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

AY–2
Automated Recovery

The TCB shall enforce an approved recovery policy. The policy shall define the product failures and service discontinuities from which recovery is possible in a trusted manner.

After a product failures or service discontinuity, **the TCB shall be able to determine whether its automated procedures can be used to return the product to normal operation in a trusted manner.**

If the automated means can be used, the TCB shall be able to perform the necessary procedures and return the product to normal operation.

If automated recovery is not used, the TCB shall enter a state where only administrators, and users to whom the required authority has been delegated, are capable of returning the product to normal operation.

Manual procedures shall be provided by which the product can be returned to normal operation in a trusted manner.

Thresholds at which discontinuities require that the product be re-installed shall be identified.

CONSTRAINT: IS-1

AY–3
Selective Recovery

The TCB shall enforce an approved recovery policy. The policy shall define the product failures and service discontinuities from which recovery is possible in a trusted manner.

After any service discontinuity, or product failure not requiring re-installation or component replacement, the TCB shall be able to perform automated recovery in a trusted manner to, at worst, a degraded mode of operation.

If automated recovery is not used, the TCB shall enter a state where only administrators, and users to whom the required authority has been delegated, are capable of returning the product to normal operation.

Manual procedures shall be provided by which the product can be returned to normal operation from a degraded mode of operation in a trusted manner.

Thresholds at which service discontinuities require that the product be re-installed shall be identified.

CONSTRAINT: IS-1

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

Accountability Criteria

A product which is rated against the Accountability Criteria must provide services capable of attributing responsibility for an action to a user. Accountability may be provided in a product through the use of *audit* services, *identification & authentication* services, and *trusted path* services.

Audit

Audit services allow the monitoring of potentially suspicious activity on the product. The Audit levels of service rate the service based on the granularity of auditing, the complexity of audit analysis tools and the ability to detect potential violations.

Appendix I provides guidance on audit trail content.

WA–0
Non-compliant

This level is reserved for those product which have been evaluated under the Audit service and have failed to meet the requirements of a higher level of service.

WA–1
External Audit

The TCB shall enforce an approved audit policy. The policy shall define the set of auditable events that can be included in the audit trail.

The TCB shall be able to perform basic auditing of security relevant events and shall be capable of providing the audit trail, via some protected mechanism, to another product or system.

The audit trail shall contain information pertaining to the date, time, location, type and success or failure of each audited event.

The audit trail shall contain sufficient information to recover the identity of the users, processes and/or objects involved in each audited event.

CONSTRAINT: WI-1

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

WA–2
Security Audit

The TCB shall enforce an approved audit policy. The policy shall define the set of auditable events that can be included in the audit trail.

The TCB shall be able to perform basic auditing of security relevant events and shall **maintain and protect the audit trail from unauthorized access, modification or destruction.**

The audit trail shall contain information pertaining to the date, time, location, type and success or failure of each audited event.

The audit trail shall contain sufficient information to recover the identity of the users, processes and/or objects involved in each audited event.

Audit review tools shall be available to administrators, and users to whom the required authority has been delegated, to assist in the inspection of the audit trail.

CONSTRAINT: IS-1, WI-1

WA–3
Security Audit & Alarm

The TCB shall enforce an approved audit policy. The policy shall define the set of auditable events that can be included in the audit trail.

The TCB shall be able to perform basic auditing of security relevant events and shall maintain and protect the audit trail from unauthorized access, modification or destruction.

The audit trail shall contain information pertaining to the date, time, location, type and success or failure of each audited event.

The audit trail shall contain sufficient information to recover the identity of the users, processes and/or objects involved in each audited event.

Audit review tools shall be available to administrators, and users to whom the required authority has been delegated, to assist in the inspection of the audit trail.

The TCB shall be able to monitor the occurrence or accumulation of auditable events that may indicate an imminent violation of the product's security policy.

The TCB shall be able to immediately notify the administrator when thresholds are exceeded and, if the occurrence or accumulation of monitored security relevant events continues, the TCB shall be able to take the least disruptive action to terminate the recurrence of these events.

CONSTRAINT: IS-1, WI-1

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

WA–4
Detailed Audit

The TCB shall enforce an approved audit policy. The policy shall define the set of auditable events that can be included in the audit trail.

The TCB shall be able to perform **detailed** auditing of security relevant events and shall maintain and protect the audit trail from unauthorized access, modification or destruction.

The audit trail shall contain information pertaining to the date, time, location, type and success or failure of each audited event.

The audit trail shall contain sufficient information to recover the identity of the users, processes and/or objects involved in each audited event.

Audit **analysis** tools shall be available to administrators, and users to whom the required authority has been delegated, to assist in the **analysis** of the audit trail.

The TCB shall be able to monitor the occurrence or accumulation of auditable events that may indicate an imminent violation of the product's security policy.

The TCB shall be able to immediately notify the administrator when thresholds are exceeded and, if the occurrence or accumulation of monitored security relevant events continues, the TCB shall be able to take the least disruptive action to terminate the recurrence of these events.

CONSTRAINT: IS-1, WI-1

WA–5
Advanced Detection

The TCB shall enforce an approved audit policy. The policy shall define the set of auditable events that can be included in the audit trail.

The TCB shall be able to perform detailed auditing of security relevant events and shall maintain and protect the audit trail from unauthorized access, modification or destruction.

The audit trail shall contain information pertaining to the date, time, location, type and success or failure of each audited event.

The audit trail shall contain sufficient information to recover the identity of the users, processes and/or objects involved in each audited event.

Audit analysis tools shall be available to administrators, and users to whom the required authority has been delegated, to assist in the analysis of the audit trail.

The TCB shall be able to monitor the occurrence or accumulation of auditable events that may indicate an imminent violation of the product's security policy.

The TCB shall be able to immediately notify the administrator when thresholds are exceeded and, if the occurrence or accumulation of monitored security relevant events continues, the TCB shall be able to take the least disruptive action to terminate the recurrence of these events.

The TCB shall be able to perform real-time intrusion detection analysis in support of the product's security policy.

CONSTRAINT: IS-1, WI-1

Identification and Authentication

Identification and Authentication services allow the TCB to verify the identity of individuals attempting access to the product. The Identification and Authentication levels of service rate these services based the number of approved authentication mechanisms available.

Appendix I provides guidance on identification and authentication mechanisms, and distinguishes between acceptable means of authentication.

WI–0
Non-compliant

This level is reserved for those products which have been evaluated under the Identification and Authentication service and have failed to meet the requirements of a higher level of service.

WI-1
External I&A

The TCB shall enforce an approved identification and authentication policy. The policy shall identify the attributes to be associated with a user and the other product services to which these attributes will be provided.

Each user shall be uniquely identified to the TCB.

The TCB shall use a protected mechanism to receive the authenticated user identity from some external source before allowing that user to perform any other TCB-mediated action.

CONSTRAINT: None

WI–2
Individual I&A

The TCB shall enforce an approved identification and authentication policy. The policy shall identify the attributes to be associated with a user and the other product services to which these attributes will be provided.

Each user shall be uniquely identified to the TCB.

The TCB shall use **a protected mechanism to authenticate each user** before allowing that user to perform any other TCB-mediated action.

The TCB shall protect authentication data from unauthorized users.

CONSTRAINT: None.

WI–3
Multiple I&A

The TCB shall enforce an approved identification and authentication policy. The policy shall identify the attributes to be associated with a user and the other product services to which these attributes will be provided.

Each user shall be uniquely identified to the TCB.

The TCB shall use **two or more different types of** protected mechanisms to authenticate each user before allowing that user to perform any other TCB-mediated action.

The TCB shall protect authentication data from unauthorized users.

CONSTRAINT: None.

Trusted Path

Trusted path services provide the ability to ensure users direct communication with the TCB. The Trusted Path levels of service rate these services based on their flexibility in allowing the TCB or the user to initiate trusted exchanges.

WT–0
Non-compliant

This level is reserved for those product which have been evaluated under the Trusted Path service and have failed to meet the requirements of a higher level of service.

WT–1
Basic Trusted Path

The TCB shall enforce an approved trusted path policy. The policy shall define a mechanism for creating a trusted communication path between the user and the TCB.

The trusted path shall be used for initial identification and authentication.

Communications via this path shall be initiated exclusively by the user.

CONSTRAINT: WI-2

WT–2
Advanced Trusted Path

The TCB shall enforce an approved trusted path policy. The policy shall define a mechanism for creating a trusted communication path between the user and the TCB.

The trusted path shall be used for initial identification and authentication**, and at other times when direct user-TCB or TCB-user communication is required.**

Trusted path exchanges originating from the TCB shall be uniquely identifiable as such, and shall require positive confirmation from the user.

CONSTRAINT: WI-2

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

T-0 — Non Compliant

Assurance Criteria

Each evaluated product must be rated against the Assurance Criteria to assess the level of trust which may be placed in it. The Assurance Criteria include requirements for Architecture, Development Environment, Development Evidence, Operational Enviroment, Security Manuals and Security Testing.

Appendix J provides guidance on meeting the Assurance Criteria requirements, and discusses assurance issues involved in the design, implementation, and evaluation of trusted products.

T-0 — Non Compliant

This level is reserved for those products that have been evaluated under the Assurance criteria but have failed to meet the requirements for a higher level.

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

Assurance Level T-1

Architecture

All TCB elements shall be identified.

The TCB shall enforce the product's security policy.

The TCB shall maintain a domain for its own execution that protects it from external interference and tampering.

Access to any resource under the control of the TCB shall only occur through the TCB interface.

Development Environment

Life Cycle Process.

The Vendor shall state the development methodology used during the life cycle of the product.

Configuration Management.

A configuration management system shall be in place during the entire life cycle of the product, and shall maintain control of changes to all hardware, firmware, source code, object code, test suites, and documentation.

The configuration management system shall assure a consistent mapping among all documentation and code associated with the current version of the TCB.

Development Evidence

Functional Specification.

The Vendor shall provide a functional specification for the product.

The functional specification shall include the informal security policy enforced by the TCB. The security policy shall state the security services provided by the TCB.

Architectural Design.

The Vendor shall provide an informal architectural design of the product.

The architectural design shall state the general structure of the product and shall identify the product's security enforcing functions.

The TCB's external interfaces shall be stated.

Any security services provided by the underlying hardware, firmware, or other software, to the product under evaluation shall be stated.

Detailed Design.

The Vendor shall provide an informal detailed design of the product.

The detailed design shall identify all security mechanisms within the TCB and shall state specifically how each security mechanism functions.

The interfaces between all TCB modules shall be documented stating their purpose and parameters.

The Vendor shall trace the complete mapping between the security policy and the detailed design.

Operational Environment

The Vendor shall provide a means for the secure installation, generation and start-up of the product.

The Vendor shall identify all configuration options which may be used during secure installation, generation and start-up of the product.

Security Manuals

Security Features User's Guide.

The Vendor shall provide a Security Features User's Guide in the form of a single summary, chapter, or manual in user documentation which describes the product's security services and provides guidelines on their use by nonadministrative users.

The Security Features User's Guide shall describe the interaction between security services.

Trusted Facility Manual.

The Vendor shall provide a Trusted Facility Manual intended for the product administrator which describes the proper administration of the product's security services.

The Trusted Facility Manual shall describe the administrative interaction between security services.

The Trusted Facility Manual shall describe the means for the secure installation, generation and start-up of the product.

The Trusted Facility Manual shall describe all configuration options which may be used during secure installation, generation and start-up of the product.

The Trusted Facility Manual shall not be included in nonadministrative user documentation.

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

Assurance Level T-1

Security Testing

The Vendor shall provide a security test plan to the Evaluation Team. The security test plan shall describe the philosophy and approach taken by the Vendor to test all of the security services provided and enforced by the TCB. The test coverage shall also be included and justified.

The Vendor shall provide evidence of security testing to the Evaluation Team in the form of a detailed set of security test procedures and corresponding security test results. This evidence must be provided in sufficient detail to allow the Vendor's security testing to be duplicated by the Evaluation Team.

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

Assurance Level T-2

Architecture

All TCB elements shall be identified.

The TCB shall enforce the product's security policy.

The TCB shall maintain a domain for its own execution that protects it from external interference and tampering.

Access to any resource under the control of the TCB shall only occur through the TCB interface.

The TCB shall maintain process isolation.

Development Environment

Life Cycle Process.

The Vendor shall **describe** the development methodology used during the life cycle of the product.

Configuration Management.

A configuration management system shall be in place during the entire life cycle of the product, and shall maintain control of changes to all hardware, firmware, source code, object code, test suites, and documentation.

The configuration management system shall assure a consistent mapping among all documentation and code associated with the current version of the TCB.

Development Evidence

Functional Specification.

The Vendor shall provide a functional specification for the product.

The functional specification shall include the informal security policy enforced by the TCB. The security policy shall **describe** the security services provided by the TCB.

The functional specification shall also include an informal security policy model.

The Vendor shall trace the complete mapping between the security policy model and the security policy. The trace shall show that the security policy model is sufficient to enforce the security policy.

Architectural Design.

The Vendor shall provide an informal architectural design of the product.

The architectural design shall **describe** the general structure of the product and shall identify the product's security enforcing functions.

The TCB's external interfaces shall be **described**.

DRAFT DRAFT DRAFT DRAFT DRAFT

Operational Environment

Security Manuals

Assurance Criteria

Any security services provided by the underlying hardware, firmware, or other software, to the product under evaluation shall be **described**.

The Vendor shall trace the complete mapping between the security policy model and the architectural design.

Detailed Design.

The Vendor shall provide an informal detailed design of the product.

The detailed design shall identify all security mechanisms within the TCB and shall **describe** specifically how each security mechanism functions.

The interfaces between all TCB modules shall be documented stating their purpose and parameters.

The Vendor shall trace the complete mapping between the security policy **model** and the detailed design.

The Vendor shall provide a means for the secure installation, generation and start-up of the product.

The Vendor shall identify all configuration options which may be used during secure installation, generation and start-up of the product.

Security Features User's Guide.

The Vendor shall provide a Security Features User's Guide in the form of a single summary, chapter, or manual in user documentation which describes the product's security services and provides guidelines on their use by nonadministrative users.

The Security Features User's Guide shall describe the interaction between security services.

Trusted Facility Manual.

The Vendor shall provide a Trusted Facility Manual intended for the product administrator which describes the proper administration of the product's security services.

The Trusted Facility Manual shall describe the administrative interaction between security services.

The Trusted Facility Manual shall describe the means for the secure installation, generation and start-up of the product.

The Trusted Facility Manual shall describe all configuration options which may be used during secure installation, generation and start-up of the product.

The Trusted Facility Manual shall not be included in nonadministrative user documentation.

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

Assurance Level T-2

Security Testing

The Vendor shall provide a security test plan to the Evaluation Team. The security test plan shall describe the philosophy and approach taken by the Vendor to test all of the security services provided and enforced by the TCB. The test coverage shall also be included and justified.

The Vendor shall provide evidence of security testing to the Evaluation Team in the form of a detailed set of security test procedures and corresponding security test results. This evidence must be provided in sufficient detail to allow the Vendor's security testing to be duplicated by the Evaluation Team.

The Vendor shall remove or neutralize all identified flaws, and the TCB shall be tested again to ensure that the identified flaws have been eliminated and that new flaws have not been introduced.

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

Assurance Level T-3

Architecture

All TCB elements shall be identified.

The TCB shall enforce the product's security policy.

The TCB shall maintain a domain for its own execution that protects it from external interference and tampering.

The TCB shall use any protection mechanisms available in the underlying abstract machine to separate protection-critical elements from non protection-critical elements.

Access to any resource under the control of the TCB shall only occur through the TCB interface.

The TCB shall maintain process isolation.

The TCB shall be internally structured into well-defined largely independent modules. Each module shall be designed such that the principle of least privilege is enforced.

Development Environment

Life Cycle Process.

The Vendor shall describe the life cycle process used during the development of the product.

The Vendor shall describe coding standards to be followed during the implementation of the product and shall ensure that all source code complies with these standards.

Any programming languages used for implementation shall be well-defined. Any implementation dependent options of the programming language or compilers shall be documented.

Configuration Management.

A configuration management system shall be in place during the entire life cycle of the product, and shall maintain control of changes to all hardware, firmware, source code, object code, test suites, and documentation.

The configuration management system shall assure a consistent mapping among all documentation and code associated with the current version of the TCB.

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

Development Evidence

Functional Specification.

The Vendor shall provide a functional specification for the product.

The functional specification shall include the informal security policy enforced by the TCB. The security policy shall describe the security services provided by the TCB.

The functional specification shall also include a **semiformal** security policy model.

The Vendor shall trace the complete mapping between the security policy model and the security policy. The trace shall show that the security policy model is sufficient to enforce the security policy.

Architectural Design.

The Vendor shall provide a **semiformal** architectural design of the product.

The architectural design shall describe the general structure of the product and shall identify the product's security enforcing functions.

The TCB's external interfaces shall be described.

Any security services provided by the underlying hardware, firmware, or other software, to the product under evaluation shall be described.

The Vendor shall trace the complete mapping between the security policy model and the architectural design.

Detailed Design.

The Vendor shall provide a **semiformal** detailed design of the product.

The detailed design shall identify all security mechanisms within the TCB and shall describe specifically how each security mechanism functions.

The interfaces between all TCB modules shall be documented stating their purpose and parameters.

The Vendor shall trace the complete mapping between the security policy model and the detailed design. **The Vendor shall also trace the complete mapping between the detailed design and the TCB implementation.**

Operational Environment

A combination of technical, procedural or physical safeguards shall exist for ensuring that the TCB software and firmware distributed to a customer are exactly as specified by the master copies.

The Vendor shall provide a means for the secure installation, generation and start-up of the product.

The Vendor shall identify all configuration options which may be used during secure installation, generation and start-up of the product.

Security Manuals

Security Features User's Guide.

The Vendor shall provide a Security Features User's Guide in the form of a single summary, chapter, or manual in user documentation which describes the product's security services and provides guidelines on their use by nonadministrative users.

The Security Features User's Guide shall describe the interaction between security services.

Trusted Facility Manual.

The Vendor shall provide a Trusted Facility Manual intended for the product administrator which describes the proper administration of the product's security services.

The Trusted Facility Manual shall describe the administrative interaction between security services.

The Trusted Facility Manual shall describe the means for the secure installation, generation and start-up of the product.

The Trusted Facility Manual shall describe all configuration options which may be used during secure installation, generation and start-up of the product.

The Trusted Facility Manual shall not be included in nonadministrative user documentation.

Security Testing

The Vendor shall provide a security test plan to the Evaluation Team. The security test plan shall describe the philosophy and approach taken by the Vendor to test all of the security services provided and enforced by the TCB. The test coverage shall also be included and justified.

The Vendor shall provide evidence of security testing to the Evaluation Team in the form of a detailed set of security test procedures and corresponding security test results. This evidence must be provided in sufficient detail to allow the Vendor's security testing to be duplicated by the Evaluation Team.

The Vendor shall remove or neutralize all identified flaws, and the TCB shall be tested again to ensure that the identified flaws have been eliminated and that new flaws have not been introduced.

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

Assurance Level T-4

Architecture

All TCB elements shall be identified.

The TCB shall enforce the product's security policy.

The TCB shall maintain a domain for its own execution that protects it from external interference and tampering.

Protection mechanisms shall be available in the underlying abstract machine. The TCB shall use these protection mechanisms to separate protection-critical elements from non protection-critical elements.

Access to any resource under the control of the TCB shall only occur through the TCB interface.

The TCB shall maintain process isolation.

The TCB shall be internally structured into well-defined largely independent modules. Each module shall be designed such that the principle of least privilege is enforced.

Development Environment

Life Cycle Process.

The Vendor shall describe the life cycle process used during the development of the product.

The Vendor shall describe coding standards to be followed during the implementation of the product and shall ensure that all source code complies with these standards.

Any programming languages used for implementation shall be well-defined. Any implementation dependent options of the programming language or compilers shall be documented.

Physical, procedural, personnel, and other security measures used by the Vendor to protect the product and its documentation shall be described.

Configuration Management.

A **tool based** configuration management system shall be in place during the entire life cycle of the product, and shall maintain control of changes to all hardware, firmware, source code, object code, test suites, and documentation.

The configuration management system shall assure a consistent mapping among all documentation and code associated with the current version of the TCB.

The configuration management system shall provide for the generation of the TCB from source code, and shall provide for the comparison of TCB versions in order to ascertain all changes.

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

Development Evidence

Assurance Criteria

The configuration management system shall be capable of tracing problem reports and affected configuration items to problem resolution.

Functional Specification.

The Vendor shall provide a functional specification for the product.

The functional specification shall include the informal security policy enforced by the TCB. The security policy shall describe the security services provided by the TCB.

The functional specification shall also include a **formal** security policy model.

The Vendor shall **demonstrate** the complete mapping between the security policy model and the security policy. The **demonstration** shall show that the security policy model is sufficient to enforce the security policy.

Architectural Design.

The Vendor shall provide a semiformal architectural design of the product.

The architectural design shall describe the general structure of the product and shall identify the product's security enforcing functions.

The TCB's external interfaces shall be described **in terms of exceptions, error messages, and effects**.

Any security services provided by the underlying hardware, firmware, or other software, to the product under evaluation shall be described.

The Vendor shall trace the complete mapping between the security policy model and the architectural design.

Detailed Design.

The Vendor shall provide a semiformal detailed design of the product.

The detailed design shall identify all security mechanisms within the TCB and shall describe specifically how each security mechanism functions.

The interfaces between all TCB modules shall be documented stating their purpose and parameters.

The Vendor shall trace the complete mapping between the **architectural design** and the detailed design. The Vendor shall also trace the complete mapping between the detailed design and the TCB implementation.

Operational Environment

A combination of technical, procedural or physical safeguards shall exist for ensuring that the TCB software and firmware distributed to a customer are exactly as specified by the master copies.

The Vendor shall provide a means for the secure installation, generation and start-up of the product.

The Vendor shall identify all configuration options which may be used during secure installation, generation and start-up of the product.

Security Manuals

Security Features User's Guide.

The Vendor shall provide a Security Features User's Guide in the form of a single summary, chapter, or manual in user documentation which describes the product's security services and provides guidelines on their use by nonadministrative users.

The Security Features User's Guide shall the describe interaction between security services.

Trusted Facility Manual.

The Vendor shall provide a Trusted Facility Manual intended for the product administrator which describes the proper administration of the product's security services.

The Trusted Facility Manual shall describe the administrative interaction between security services.

The Trusted Facility Manual shall describe the means for the secure installation, generation and start-up of the product.

The Trusted Facility Manual shall describe all configuration options which may be used during secure installation, generation and start-up of the product.

The Trusted Facility Manual shall not be included in nonadministrative user documentation.

Security Testing

The Vendor shall provide a security test plan to the Evaluation Team. The security test plan shall describe the philosophy and approach taken by the Vendor to test all of the security services provided and enforced by the TCB. The test coverage shall also be included and justified.

The Vendor shall provide evidence of security testing to the Evaluation Team in the form of a detailed set of security test procedures and corresponding security test results. This evidence must be provided in sufficient detail to allow the Vendor's security testing to be duplicated by the Evaluation Team.

The Vendor shall **correct** all identified flaws, and the TCB shall be tested again to ensure that the identified flaws have been eliminated and that new flaws have not been introduced.

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

Assurance Criteria

The TCB shall be found relatively resistant to penetration by the Vendor.

The Vendor shall demonstrate that the TCB implementation is consistent with the Detailed Design.

Assurance Level T-5

Architecture

All TCB elements shall be identified.

The TCB shall enforce the product's security policy.

The TCB shall maintain a domain for its own execution that protects it from external interference and tampering.

Protection mechanisms shall be available in the underlying abstract machine. The TCB shall use these protection mechanisms to separate protection-critical elements from non protection-critical elements.

Access to any resource under the control of the TCB shall only occur through the TCB interface.

The TCB shall maintain process isolation.

The TCB shall be internally structured into well-defined largely independent modules. Each module shall be designed such that the principle of least privilege is enforced. **An effort shall be made by the Vendor to exclude modules from the TCB which are not protection-critical. Rationale for the inclusion of any protection-irrelevant elements in the TCB shall be provided.**

Significant software engineering shall be directed toward minimizing the complexity of the TCB. The TCB shall be designed and structured to use a complete, conceptually simple protection mechanism with precisely defined semantics. This mechanism shall play a central role in enforcing the internal structuring of the TCB and the product. The TCB shall incorporate significant use of layering, abstraction and data hiding.

Development Environment

Life Cycle Process.

The Vendor shall describe the life cycle process used during the development of the product.

The Vendor shall describe coding standards to be followed during the implementation of the product and shall ensure that all source code complies with these standards.

Any programming languages used for implementation shall be well-defined. Any implementation dependent options of the programming language or compilers shall be documented.

Physical, procedural, personnel, and other security measures used by the Vendor to protect the product and its documentation shall be described.

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

Development Evidence

Configuration Management.

A tool based configuration management system shall be in place during the entire life cycle of the product, and shall maintain control of changes to all hardware, firmware, source code, object code, test suites, and documentation.

The configuration management system shall assure a consistent mapping among all documentation and code associated with the current version of the TCB.

The configuration management system shall provide for the generation of the TCB from source code, and shall provide for the comparison of TCB versions in order to ascertain all changes.

The configuration management system shall be capable of tracing problem reports and affected configuration items to problem resolution.

Functional Specification.

The Vendor shall provide a functional specification for the product.

The functional specification shall include the informal security policy enforced by the TCB. The security policy shall describe the security services provided by the TCB.

The functional specification shall also include a formal security policy model.

The Vendor shall demonstrate the complete mapping between the security policy model and the security policy. The demonstration shall show that the security policy model is sufficient to enforce the security policy.

Architectural Design.

The Vendor shall provide a semiformal architectural design of the product.

The architectural design shall **explain** the general structure of the product and shall identify the product's security enforcing functions.

The TCB's external interfaces shall be **explained** in terms of exceptions, error messages, and effects.

Any security services provided by the underlying hardware, firmware, or other software, to the product under evaluation shall be **explained**.

The Vendor shall **demonstrate** the complete mapping between the security policy model and the architectural design.

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

Operational Environment

Detailed Design.

The Vendor shall provide a semiformal detailed design of the product.

The detailed design shall identify all security mechanisms within the TCB and shall **explain** specifically how each security mechanism functions.

The interfaces between all TCB modules shall be documented stating their purpose and parameters.

The Vendor shall trace the complete mapping between the architectural design and the detailed design. The Vendor shall also trace the complete mapping between the detailed design and the TCB implementation.

A combination of technical, procedural or physical safeguards shall exist for ensuring that the TCB software and firmware distributed to a customer are exactly as specified by the master copies.

The Vendor shall provide a means for the secure installation, generation and start-up of the product.

The Vendor shall identify all configuration options which may be used during secure installation, generation and start-up of the product.

Security Manuals

Security Features User's Guide.

The Vendor shall provide a Security Features User's Guide in the form of a single summary, chapter, or manual in user documentation which describes the product's security services and provides guidelines on their use by nonadministrative users.

The Security Features User's Guide shall describe the interaction between security services.

Trusted Facility Manual.

The Vendor shall provide a Trusted Facility Manual intended for the product administrator which describes the proper administration of the product's security services.

The Trusted Facility Manual shall describe the administrative interaction between security services.

The Trusted Facility Manual shall describe the means for the secure installation, generation and start-up of the product.

The Trusted Facility Manual shall describe all configuration options which may be used during secure installation, generation and start-up of the product.

The Trusted Facility Manual shall not be included in nonadministrative user documentation.

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

Assurance Criteria

Security Testing

The Vendor shall provide a security test plan to the Evaluation Team. The security test plan shall describe the philosophy and approach taken by the Vendor to test all of the security services provided and enforced by the TCB. The test coverage shall also be included and justified.

The Vendor shall provide evidence of security testing to the Evaluation Team in the form of a detailed set of security test procedures and corresponding security test results. This evidence must be provided in sufficient detail to allow the Vendor's security testing to be duplicated by the Evaluation Team.

The Vendor shall correct all identified flaws, and the TCB shall be tested again to ensure that the identified flaws have been eliminated and that new flaws have not been introduced.

The TCB shall be found resistant to penetration by the Vendor.

No design flaws and no more than a few correctable implementation flaws may be found during testing.

The Vendor shall demonstrate that the TCB implementation is consistent with the Detailed Design.

Assurance Level T-6

Architecture

All TCB elements shall be identified.

The TCB shall enforce the product's security policy.

The TCB shall maintain a domain for its own execution that protects it from external interference and tampering.

Protection mechanisms shall be available in the underlying abstract machine. The TCB shall use these protection mechanisms to separate protection-critical elements from non protection-critical elements.

Access to any resource under the control of the TCB shall only occur through the TCB interface.

The TCB shall maintain process isolation.

The TCB shall be internally structured into well-defined largely independent modules. Each module shall be designed such that the principle of least privilege is enforced. An effort shall be made by the Vendor to exclude modules from the TCB which are not protection-critical. Rationale for the inclusion of any protection-irrelevant elements in the TCB shall be provided.

Significant software engineering shall be directed toward minimizing the complexity of the TCB. The TCB shall be designed and structured to use a complete, conceptually simple protection mechanism with precisely defined semantics. This mechanism shall play a central role in enforcing the internal structuring of the TCB and the product. The TCB shall incorporate significant use of layering, abstraction and data hiding.

Development Environment

Life Cycle Process.

The Vendor shall describe the life cycle process used during the development of the product.

The Vendor shall describe coding standards to be followed during the implementation of the product and shall ensure that all source code complies with these standards.

Any programming languages used for implementation shall be well-defined. Any implementation dependent options of the programming language or compilers shall be documented.

Source code of any runtime libraries shall be provided.

Physical, procedural, personnel, and other security measures used by the Vendor to protect **development tools,** the product and its documentation shall be described.

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

Development Evidence

Configuration Management.

A tool based configuration management system shall be in place during the entire life cycle of the product, and shall maintain control of changes to all **development tools,** hardware, firmware, source code, object code, test suites, and documentation.

The configuration management system shall assure a consistent mapping among all documentation and code associated with the current version of the TCB.

The configuration management system shall provide for the generation of the TCB from source code, and shall provide for the comparison of TCB versions in order to ascertain all changes.

The configuration management system shall be capable of tracing problem reports and affected configuration items to problem resolution.

A combination of technical, physical, and procedural safeguards shall be used to protect from an unauthorized modification or destruction the master copy or copies of all material used to generate the TCB.

Functional Specification.

The Vendor shall provide a functional specification for the product.

The functional specification shall include the informal security policy enforced by the TCB. The security policy shall describe the security services provided by the TCB.

The functional specification shall also include a formal security policy model.

The Vendor shall demonstrate the complete mapping between the security policy model and the security policy. The demonstration shall show that the security policy model is sufficient to enforce the security policy.

Architectural Design.

The Vendor shall provide a **formal (and semiformal where necessary)** architectural design of the product.

The architectural design shall explain the general structure of the product and shall identify the product's security enforcing functions.

The TCB's external interfaces shall be explained in terms of exceptions, error messages, and effects.

Any security services provided by the underlying hardware, firmware, or other software, to the product under evaluation shall be explained.

The Vendor shall **prove** the complete mapping between the security policy model and the architectural design.

Detailed Design.

The Vendor shall provide a semiformal detailed design of the product.

The detailed design shall identify all security mechanisms within the TCB and shall explain specifically how each security mechanism functions.

The interfaces between all TCB modules shall be documented stating their purpose and parameters.

The Vendor shall **demonstrate** the complete mapping between the architectural design and the detailed design. The Vendor shall also trace the complete mapping between the detailed design and the TCB implementation.

Operational Environment

A trusted product control and distribution facility shall be provided for maintaining the mapping between the TCB distributed to a customer and the master copies.

A combination of technical, procedural or physical safeguards shall exist for ensuring that the TCB software and firmware distributed to a customer are exactly as specified by the master copies.

The Vendor shall provide a means for the secure installation, generation and start-up of the product.

The Vendor shall identify all configuration options which may be used during secure installation, generation and start-up of the product.

Security Manuals

Security Features User's Guide.

The Vendor shall provide a Security Features User's Guide in the form of a single summary, chapter, or manual in user documentation which describes the product's security services and provides guidelines on their use by nonadministrative users.

The Security Features User's Guide shall describe the interaction between security services.

Trusted Facility Manual.

The Vendor shall provide a Trusted Facility Manual intended for the product administrator which describes the proper administration of the product's security services.

The Trusted Facility Manual shall describe the administrative interaction between security services.

The Trusted Facility Manual shall describe the means for the secure installation, generation and start-up of the product.

The Trusted Facility Manual shall describe all configuration options which may be used during secure installation, generation and start-up of the product.

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

Security Testing

The Trusted Facility Manual shall not be included in nonadministrative user documentation.

The Vendor shall provide a security test plan to the Evaluation Team. The security test plan shall describe the philosophy and approach taken by the Vendor to test all of the security services provided and enforced by the TCB. The test coverage shall also be included and justified.

The Vendor shall provide evidence of security testing to the Evaluation Team in the form of a detailed set of security test procedures and corresponding security test results. This evidence must be provided in sufficient detail to allow the Vendor's security testing to be duplicated by the Evaluation Team.

The Vendor shall correct all identified flaws, and the TCB shall be tested again to ensure that the identified flaws have been eliminated and that new flaws have not been introduced.

The TCB shall be found resistant to penetration by the Vendor.

No design flaws and no more than a few correctable implementation flaws may be found during testing.

The Vendor shall demonstrate that the TCB implementation is consistent with **the Architectural Design and** the Detailed Design.

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

Assurance Level T-7

Architecture

All TCB elements shall be identified.

The TCB shall enforce the product's security policy.

The TCB shall maintain a domain for its own execution that protects it from external interference and tampering.

Protection mechanisms shall be available in the underlying abstract machine. The TCB shall use these protection mechanisms to separate protection-critical elements from non protection-critical elements.

Access to any resource under the control of the TCB shall only occur through the TCB interface.

The TCB shall maintain process isolation.

The TCB shall be internally structured into well-defined largely independent modules. Each module shall be designed such that the principle of least privilege is enforced. An effort shall be made by the Vendor to exclude modules from the TCB which are not protection-critical. Rationale for the inclusion of any protection-irrelevant elements in the TCB shall be provided.

Significant software engineering shall be directed toward minimizing the complexity of the TCB. The TCB shall be designed and structured to use a complete, conceptually simple protection mechanism with precisely defined semantics. This mechanism shall play a central role in enforcing the internal structuring of the TCB and the product. The TCB shall incorporate significant use of layering, abstraction and data hiding.

Development Environment

Life Cycle Process.

The Vendor shall describe the life cycle process used during the development of the product.

The Vendor shall describe coding standards to be followed during the implementation of the product and shall ensure that all source code complies with these standards.

Any programming languages used for implementation shall be well-defined. Any implementation dependent options of the programming language or compilers shall be documented.

Source code of any runtime libraries shall be provided.

Physical, procedural, personnel, and other security measures used by the Vendor to protect development tools, the product and its documentation shall be described.

Configuration Management.

A tool based configuration management system shall be in place during the entire life cycle of the product, and shall maintain control of changes to all development tools, hardware, firmware, source code, object code, test suites, and documentation.

The configuration management system shall assure a consistent mapping among all documentation and code associated with the current version of the TCB.

The configuration management system shall provide for the generation of the TCB from source code, and shall provide for the comparison of TCB versions in order to ascertain all changes.

The configuration management system shall be capable of tracing problem reports and affected configuration items to problem resolution.

A combination of technical, physical, and procedural safeguards shall be used to protect from an unauthorized modification or destruction the master copy or copies of all material used to generate the TCB.

Development Evidence

Functional Specification.

The Vendor shall provide a functional specification for the product.

The functional specification shall include the informal security policy enforced by the TCB. The security policy shall describe the security services provided by the TCB.

The functional specification shall also include a formal security policy model.

The Vendor shall demonstrate the complete mapping between the security policy model and the security policy. The demonstration shall show that the security policy model is sufficient to enforce the security policy.

Architectural Design.

The Vendor shall provide a **formal** architectural design of the product.

The architectural design shall explain the general structure of the product and shall identify the product's security enforcing functions.

The TCB's external interfaces shall be explained in terms of exceptions, error messages, and effects.

Any security services provided by the underlying hardware, firmware, or other software, to the product under evaluation shall be explained.

The Vendor shall prove the complete mapping between the security policy model and the architectural design.

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

Operational Environment

Detailed Design.

The Vendor shall provide a **formal** detailed design of the product.

The detailed design shall identify all security mechanisms within the TCB and shall explain specifically how each security mechanism functions.

The interfaces between all TCB modules shall be documented stating their purpose and parameters.

The Vendor shall **prove** the complete mapping between the architectural design and the detailed design. The Vendor shall also **demonstrate** the complete mapping between the detailed design and the TCB implementation.

A trusted product control and distribution facility shall be provided for maintaining the mapping between the TCB distributed to a customer and the master copies.

A combination of technical, procedural or physical safeguards shall exist for ensuring that the TCB software and firmware distributed to a customer are exactly as specified by the master copies.

The Vendor shall provide a means for the secure installation, generation and start-up of the product.

The Vendor shall identify all configuration options which may be used during secure installation, generation and start-up of the product.

Security Manuals

Security Features User's Guide.

The Vendor shall provide a Security Features User's Guide in the form of a single summary, chapter, or manual in user documentation which describes the product's security services and provides guidelines on their use by nonadministrative users.

The Security Features User's Guide shall describe the interaction between security services.

Trusted Facility Manual.

The Vendor shall provide a Trusted Facility Manual intended for the product administrator which describes the proper administration of the product's security services.

The Trusted Facility Manual shall describe the administrative interaction between security services.

The Trusted Facility Manual shall describe the means for the secure installation, generation and start-up of the product.

The Trusted Facility Manual shall describe all configuration options which may be used during secure installation, generation and start-up of the product.

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

Security Testing

The Trusted Facility Manual shall not be included in nonadministrative user documentation.

The Vendor shall provide a security test plan to the Evaluation Team. The security test plan shall describe the philosophy and approach taken by the Vendor to test all of the security services provided and enforced by the TCB. The test coverage shall also be included and justified.

The Vendor shall provide evidence of security testing to the Evaluation Team in the form of a detailed set of security test procedures and corresponding security test results. This evidence must be provided in sufficient detail to allow the Vendor's security testing to be duplicated by the Evaluation Team.

The Vendor shall correct all identified flaws, and the TCB shall be tested again to ensure that the identified flaws have been eliminated and that new flaws have not been introduced.

The TCB shall be found resistant to penetration by the Vendor.

No design flaws and no more than a few correctable implementation flaws may be found during testing.

The Vendor shall demonstrate that the TCB implementation is consistent with the Architectural Design and the Detailed Design.

Bibliography

- Canadian System Security Centre *Proceedings from the Canadian Trusted Computer Product Evaluation Criteria Workshop.* August 4 – 5, 1988.
- Canadian System Security Centre *Proceedings of the 1990 CTCPEC Availability Workshop.* February 6 – 7, 1990.
- Computer Systems Research Institute, University of Toronto *Composability of Trusted Systems.* Reports 1 – 5 [October 16, 1989, January 31, 1990, May 31, 1990, September 31, 1990, January 31, 1991]. B. Thompson, R. Soper, P.I.P. Boulton, E.S. Lee, authors.
- Department of Defense *Trusted Computer System Evaluation Criteria.* DoD 5200.28–STD, December 1985.
- Department of Defense *Magnetic Remanence Security Guideline.* DoD CSC-STD-005–85, November 15, 1985.
- National Computer Security Center *A Guide to Understanding Audit in Trusted Systems.* NCSC-TG-001, Version-2, June 1, 1988.
- National Computer Security Center *A Guide to Understanding Discretionary Access Control in Trusted Systems.* NCSC-TG-003, Version-1, September 30, 1987.
- National Computer Security Center *Trusted Network Interpretation.* NCSC-TG-005, Version-1, July 31, 1987.
- National Computer Security Center *A Guide to Understanding Configuration Management in Trusted Systems.* NCSC-TG-006, Version-1, March 28, 1988.
- National Computer Security Center *A Guide to Understanding Design Documentation in Trusted Systems.* NCSC-TG-007, Version-1, October 2, 1988.
- National Computer Security Center *Computer Security Subsystem Interpretation.* NCSC-TG-009, Version-1, September 16, 1988.
- National Computer Security Center *Rating Maintenance Phase Program Document.* NCSC-TG-013, Version-1, June 23, 1989.
- National Computer Security Center *A Guide to Understanding Object Reuse in Trusted Systems (Draft).* NCSC-TG-018, Version-1, September 15, 1989.

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

Bibliography

- National Computer Security Center *Trusted Database Management System Interpretation.* NCSC-TG-021, Version-1, April 1991.
- *Information Technology Security Evaluation Criteria.* Harmonised Criteria of France – Germany – the Netherlands – the United Kingdom. Version 1, May 2, 1990
- Zentralstelle für Sicherheit in der Informationstechnik (ZSI)*IT – Security Criteria.* Criteria for the Evaluation of Trustworthiness of Information Technology (IT) Systems. Version 1, 1989.
- U.S. Department of Commerce/National Institute of Standards and Technology *Security Requirements for Cryptographic Modules (Draft).* Federal Information Processing Standards Publication (FIPS) 140–1, July 13, 1990.
- IEEE *Proceedings of the Security and Privacy Symposium.* Oakland, California. 1980 – 1991, inclusive.
- IEEE *Proceedings of the Computer Security Applications Conference (original title: Aerospace Computer Security Applications Conference).* 1985 – 1989, inclusive.
- National Insitute of Standards and Technology *National Computer Security Conference.* 1984, 1988, 1989.
- National Institute of Standards and Technology *Report on the Invitational Workshop on Data Integrity.* NIST Special Publication 500–168, September 1989. Zella G. Ruthberg, William T. Polk editors.