COMMISSION DES COMMUNAUTÉS EUROPÉENNES

DIRECTORAT GÉNÉRAL XIII : Télécommunications, Marché de l'Information et Exploitation de la Recherche

DIRECTORAT B : Technologies et Services des Communications Avancées
B6 : Sécurité des Télécommunications et des Systèmes d'Information

Manuel d'Évaluation de la Sécurité des Technologies de l'Information

(ITSEM)

Version 1.0

Adresse : Rue de la Loi 200, B-1049 Bruxelles - Bureau Av. de Beaulieu 9 2/11 B-1160 Bruxelles
Téléphone : ligne directe (+32 2) 296 36 02, Secrétariat 296 34 19 - Fax (+32 2) 296 62 71
Courrier électronique : dhe@postman.dg13.cec.be - ISCO @postman.dg13.cec.be Compuserve 1000137.1072

A la suite d’une consultation internationale approfondie, la version 1.0 de l’ITSEM est publiée, pour un emploi opérationnel dans le cadre des schémas d’évaluation et de certification, pour une période initiale de deux ans à compter de sa date de publication. La pratique acquise sera utilisée pour réviser et approfondir l’ITSEM à la fin de la période. De plus, les considérations provenant d’une harmonisation internationale plus poussée seront prises en compte.

© ECSC-EEC-EAEC, Bruxelles - Luxembourg 1992, 1993.

La reproduction est autorisée dans le but de propagation et d’étude, pourvu que la source soit indiquée.

Table des matières

Partie 0 Introduction

Partie 1 Cadre de la sécurité des TI

Partie 2 Schémas de certification

Partie 3 Philosophie, concepts et principes

Partie 4 Processus d'évaluation

Partie 6 Conseils aux autres parties

Figures

Partie 0 Introduction

Partie 1 Cadre de la sécurité des TI

Partie 2 Schémas de certification

Partie 3 Philosophie, concepts et principes

Partie 4 Processus d'évaluation

Partie 5 Exemples d'application des ITSEC

Partie 6 Conseils aux autres parties

Partie 0 Introduction

Table des matières

Chapitre 0.1 Introduction

Contexte

0.1.1 En mai 1990, la France, l'Allemagne, les Pays-Bas et le Royaume Uni ont publié les *Critères d'Évaluation de la Sécurité des Systèmes Informatiques* [ITSEC] fondés sur les travaux à l'échelle nationale existant dans ces différents pays. Après une large relecture internationale, les ITSEC ont été améliorés par deux versions successives dont la version courante 1.2 constitue le fondement pour ce document.

0.1.2 Une raison importante pour souhaiter la production de ces critères harmonisés au plan international était qu'une telle harmonisation constitue l'une des conditions préalables à la reconnaissance mutuelle des certificats qui résument les résultats d'évaluation de la sécurité des Technologies de l'Information (TI) et qui attestent que les évaluations ont été correctement conduites. La reconnaissance mutuelle exige également que les méthodes suivies pour appliquer ces critères harmonisés soient elles-mêmes harmonisées. C'est pourquoi les quatre pays ont poursuivi leur coopération une fois les ITSEC terminés, dans le but de se mettre d'accord sur une approche commune à la conduite des évaluations de la sécurité des TI, en allant aussi loin que l'exige l'établissement de la confiance requise pour faciliter la reconnaissance mutuelle.

0.1.3 Bien des travaux sur le développement des méthodes d'évaluation de la sécurité des TI avaient déjà été réalisés et certains d'entre eux avaient été publiés. Au Royaume Uni, il s'agissait du mémorandum numéro 2 du CESG [CESG2], développé à l'usage du gouvernement, et de la série des "Livres Verts" du Ministère de l'Industrie et du Commerce, y compris le Manuel d'Évaluation et de Certification-V23 [DTI23], pour les produits de sécurité des TI commerciaux. En Allemagne, l'Agence Allemande pour la Sécurité de l'Information publiait son Manuel d'Évaluation des TI [GISA1].

0.1.4 Le principe de base était d'harmoniser suffisamment les méthodes d'évaluation de la sécurité qui existent dans chacun des quatre pays pour assurer que les méthodes d'évaluation nationales soient conformes à une philosophie unique. Initialement il semblait que le travail aurait dû se borner à l'harmonisation des méthodes existantes. Cependant, il fut nécessaire d'étendre les travaux qui existaient et de développer de nouvelles idées pour atteindre ces objectifs.

Champ d'application général

0.1.5 Ce Manuel d'Évaluation de la Sécurité des Technologies de l'Information (ITSEM) repose sur la version 1.2 des ITSEC, et décrit comment une cible d'évaluation (TOE) doit être évaluée selon ces critères. L'objectif spécifique de l'ITSEM est d'assurer qu'il existe un ensemble harmonisé de méthodes d'évaluation qui complète les ITSEC.

0.1.6 L'ITSEM est un document technique, qui s'adresse d'abord aux partenaires d'une évaluation (en premier lieu aux évaluateurs mais aussi aux commanditaires et aux organismes de certification), mais qui présente aussi un intérêt pour les fournisseurs, les développeurs, les responsables de l'homologation de système et les utilisateurs. Les méthodes et les procédures d'évaluation y sont suffisamment détaillées pour obtenir l'équivalence technique entre des évaluations conduites dans des environnements différents. Ce document sera en diffusion libre. L'ITSEM sera applicable aux évaluations

qu'elles soient menées dans les secteurs commerciaux ou dans les secteurs gouvernementaux.

0.1.7 Pour les besoins de la reconnaissance mutuelle il est nécessaire que certaines parties de l'ITSEM soient obligatoires pour les évaluateurs. Cependant, pour la plus grande part l'ITSEM est à caractère descriptif ou est prévu pour apporter des conseils.

0.1.8 Afin de donner, dans un contexte, un caractère descriptif et obligatoire aux méthodes d'évaluation, il est nécessaire de fournir dans le manuel ITSEM quelques informations générales sur la certification et sur la façon dont elle peut être organisée.

0.1.9 Ce document insiste sur l'importance de l'indépendance de l'évaluation vis-à-vis de toute pression commerciale d'un commanditaire ou d'un développeur d'une cible d'évaluation. Cependant, une évaluation "primaire", dans le sens d'une évaluation menée par une partie de l'organisation du commanditaire lui-même ou du développeur lui-même, n'est pas écartée pourvu que les exigences du schéma national soient satisfaites.

0.1.10 L'ITSEM a été écrit dans la perspective d'une évaluation en vue d'une certification. Le cas d'une évaluation suivie d'une déclaration du fournisseur est hors du champ d'application de ce document bien que l'ITSEM puisse conserver son utilité même dans ce cas.

Organisation et contenu

0.1.11 Le reste de ce document est constitué de six parties dont l'une contient des annexes. Chaque partie a été rédigée en tenant compte de l'audience visée. Certains sujets sont traités dans plusieurs parties, mais avec des niveaux de détail différents.

0.1.12 La partie 1 de l'ITSEM décrit un cadre pour la sécurité des TI qui fournit un contexte et un argumentaire sur la sécurité, l'évaluation, la certification des TI et l'homologation des systèmes. Cette partie est à caractère général et s'adresse aux responsables.

0.1.13 La partie 2 de l'ITSEM offre les informations de base sur la mise en place et le fonctionnement d'un schéma d'évaluation et de certification, en décrivant les caractéristiques générales du processus de certification et son organisation. Cette partie intéresse ceux qui désirent comprendre le processus de certification.

0.1.14 La partie 3 de l'ITSEM explique la philosophie d'évaluation qui sous-tend les critères ITSEC. Elle consigne les principes que les évaluateurs doivent suivre en conduisant les évaluations. Elle clarifie et explique plus avant les concepts des ITSEC afin de permettre une meilleure compréhension des enjeux techniques qui sous-tendent l'évaluation.

0.1.15 La partie 4 de l'ITSEM est la partie clef pour ceux qui sont impliqués dans l'évaluation. Tout le texte à caractère obligatoire se trouve dans cette partie. Elle offre un aperçu de la conduite d'évaluation et décrit l'évaluation en termes de données, d'actions et de résultats. Cependant, cette partie n'offre pas de conseils pour tous les détails de l'évaluation.

0.1.16 La partie 5 de l'ITSEM fournit des exemples de la façon dont les critères ITSEC peuvent être appliqués à l'évaluation de systèmes et de produits.

0.1.17 La partie 6 de l'ITSEM propose des conseils pour l'évaluation, destinés aux commanditaires, aux fournisseurs, aux développeurs, aux responsables de l'homologation de systèmes et aux utilisateurs. Cette partie traite plus particulièrement de la préparation des données et de l'utilisation des résultats de l'évaluation.

Numérotation et conventions typographiques

0.1.18 Chaque paragraphe d'une partie est identifié de façon unique par la combinaison du numéro de partie, du numéro de chapitre et du numéro de paragraphe dans le chapitre. La première utilisation d'un terme du glossaire de l'ITSEM dans une partie est indiquée en caractères gras. Les *caractères italiques* sont utilisés pour souligner ou pour citer. Dans la partie 4 de l'ITSEM, le texte à caractère obligatoire a été souligné en écrivant des phrases ou des paragraphes ***en gras sur fond gris***[1].

Futurs développements

0.1.19 La version 1.2 des ITSEC est actuellement utilisée pour une période d'essai. Durant cette période, des propositions sont attendues visant à l'amélioration des ITSEC à la lumière de l'expérience pratique. L'ITSEM repose aussi sur d'autres documents ([CESG2], [DTI23], [GISA1]) qui ont déjà été largement discutés et utilisés dans la pratique dans le cadre des schémas nationaux ; les rédacteurs estiment que les idées et les concepts ont été soigneusement pesés et que la structure retenue pour le document est la meilleure pour obtenir la cohérence et la facilité d'utilisation maximales.

0.1.20 La version courante de l'ITSEM bénéficie de révisions importantes qui résultent d'une large relecture internationale. Le processus de consultation s'est déroulé avec le concours de la Commission des Communautés Européennes qui a organisé une réunion internationale de travail en septembre 1992 au cours de laquelle la version 0.2 a été discutée. Cette réunion s'est accompagnée de commentaires écrits et de contributions faites par les relecteurs que les auteurs se sont efforcés de prendre en compte dans la rédaction de la version 1.0. Les auteurs de l'ITSEM reconnaissent que dans certains domaines l'ITSEM ne fournit pas encore assez de conseils détaillés ; des informations supplémentaires sur ces aspects figureront dans des versions ultérieures au fur et à mesure que ce document et les ITSEC évolueront en accord avec l'expérience.

1. NdT : pour des raisons techniques, les caractères gras sur fond gris ont été remplacés par des caractères gras et obliques dans une police de caractères différente.

Chapitre 0.2 Informations générales

Points de contact

0.2.1 Les commentaires et les suggestions sont encouragés et peuvent être envoyés à l'une des adresses ci-après, avec la mention "Commentaires sur l'ITSEM" :

Commission des Communautés Européennes
DIRECTORAT GENERAL XIII : Télécommunications, Marché de l'Information et Exploitation de la Recherche
DIRECTORAT B : Technologies et Services des Communications Avancées
Rue de la Loi 200
B-1049 BRUXELLES
Belgique

Pour la France :

Service Central de la Sécurité des Systèmes d'Information
18 rue du Docteur Zamenhof
F-92131 ISSY LES MOULINEAUX

Pour l'Allemagne :

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
D-53133 BONN

Pour les Pays-Bas :
Netherlands National Comsec Agency
Bezuidenhoutseweg 67
P.O. Box 20061
NL-2500 EB THE HAGUE

National Security Service
P.O. Box 20010
NL-2500 EA THE HAGUE

Pour le Royaume Uni :

Head of the Certification Body
UK IT Security Evaluation and Certification Scheme
Certification Body
PO Box 152
CHELTENHAM
Glos GL52 5UF

Glossaire et références

0.2.2 Le glossaire contient les définitions des termes techniques utilisés avec une signification spécifique à ce document. Les termes techniques utilisés dans le présent document qui ne sont pas définis ici sont employés dans tout le document dans un sens conforme au glossaire des ITSEC. Les termes techniques qui ne sont définis ni dans le présent glossaire ni dans le glossaire des ITSEC sont employés dans leur acception généralement admise.

Abréviations[1]

0.2.3	AGL	(PIPSE - 0.2.14)	- Atelier de génie logiciel
0.2.4	AMDE	(FMEA - 0.2.11)	- Analyse de mode de défaillances et de leurs effets
0.2.5	ANSI	(ANSI - 0.2.3)	- American National Standards Institute
0.2.6	CAO	(CAD - 0.2.4)	- Conception assistée par ordinateur
0.2.7	CESTI	(ITSEF - 0.2.17)	- Centre d'évaluation de la sécurité des technologies de l'information
0.2.8	CRC	(CRC - 0.2.7)	- Contrôle par redondance cyclique
0.2.9	DAC	(DAC - 0.2.8)	- Contrôle d'accès discrétionnaire
0.2.10	PID	(PID - 0.2.25)	- Dispositif d'identification personnelle
0.2.11	FDS	(SEF - 0.2.29)	- Fonctions dédiées à la sécurité
0.2.12	FMPS	(FMSP - 0.2.12)	- Modèle formel de politique de sécurité
0.2.13	GL	(CASE)	- Génie logiciel
0.2.14	I&A	(I&A - 0.2.13)	- Identification et authentification
0.2.15	IPSE	(IPSE - 0.2.14)	- Environnement intégre de soutien de projet
0.2.16	ISO	(ISO - 0.2.15)	- International Standards Organisation
0.2.17	ITSEC	(ITSEC - 0.2.16)	- Critères d'évaluation de la sécurité des systèmes informatiques
0.2.18	ITSEM	(ITSEM - 0.2.18)	- Manuel d'évaluation de la sécurité des technologies de l'information
0.2.19	MAC	(MAC - 0.2.19)	- Contrôle d'accès par mandats
0.2.20	MARION	(MARION - 0.2.20)	- Méthode d'analyse de risques informatiques et d'optimisation par niveau

1. NdT : à chaque terme et abréviation sont associés, entre parenthèses, le terme anglais et le numéro du paragraphe correspondant dans la version anglaise de l'ITSEM.

0.2.21	MELISA	(MELISA - 0.2.21)	- Méthode d'évaluation de la vulnérabilité résiduelle des systèmes
0.2.22	MMI	(MMI - 0.2.22)	- Interface Homme-Machine
0.2.23	OC	(CB - 0.2.6)	- Organisme de certification
0.2.24	PDL	(PDL - 0.2.24)	- Langage de description de programmes
0.2.25	PTE	(EWP - 0.2.10)	- Programme de travail pour l'évaluation
0.2.26	RdM	(SoM - 0.2.30)	- Résistance des mécanismes
0.2.27	RTE	(ETR - 0.2.9)	- Rapport technique d'évaluation
0.2.28	SEISP	(SEISP - 0.2.28)	- Politique de sécurité de l'information dans les systèmes électroniques
0.2.29	SMP	(SPM - 0.2.31)	- Modèle de politique de sécurité
0.2.30	SSADM	(SSADM - 0.2.27)	- Structured Systems Analysis and Design Methodology
0.2.31	SSP	(SSP - 0.2.32)	- Politique de sécurité d'un système
0.2.32	TCB	(TCB - 0.2.33)	- Base Informatique de Confiance
0.2.33	TOE	(TOE - 0.2.34)	- Cible d'évaluation
0.2.34	T&O	(T&T - 0.2.35)	- Technique et outil

Glossaire

0.2.35 **Analyse d'impact** (impact analysis - 0.2.50) : activité réalisée par un commanditaire pour déterminer si une réévaluation est nécessaire suite à un changement d'une cible d'évaluation.

0.2.36 **Analyse de pertinence** (suitability analysis - 0.2.66) : analyse visant à déterminer que les fonctions dédiées à la sécurité décrites dans la cible de sécurité sont en mesure de contrer les menaces identifiées dans la cible de sécurité (la pertinence n'est estimée qu'à ce niveau).

0.2.37 **Analyse de cohésion** (binding analysis - 0.2.39) : analyse visant à déterminer si la totalité des fonctions dédiées à la sécurité atteint la totalité des objectifs de sécurité, i.e. ces fonctions contrent les menaces énumérées dans la cible de sécurité, en tenant compte de la description de leurs interactions décrites dans la conception générale.

0.2.38 **Authentification** (authentication - 0.2.38) : vérification d'une identité déclarée.

0.2.39 **Bien** (asset - 0.2.36) : information ou ressource à protéger par les contre-mesures techniques et non techniques d'une cible d'évaluation.

0.2.40 **Centre d'évaluation de la sécurité des technologies de l'information** (information technology security evaluation facility - 0.2.52) : organisation accréditée selon des règles bien établies (e.g. [EN45]) et agréée par l'OC pour conduire des évaluations de la sécurité selon les ITSEC.

0.2.41 **Certificat/Rapport de certification** (certificate/certification report - 0.2.40) : document public délivré par un OC en tant que déclaration formelle confirmant les résultats de l'évaluation et que les critères, les méthodes et les procédures d'évaluation ont été correctement appliqués ; ce document comprend des détails pertinents de l'évaluation fondés sur le RTE.

0.2.42 **Contre-mesure** (countermeasure - 0.2.44) : mesure de sécurité technique ou non technique qui contribue à atteindre les objectifs de sécurité d'une cible d'évaluation.

0.2.43 **Erreur** (error - 0.2.46) : manquement à la satisfaction d'un critère de conformité.

0.2.44 **Fond de panier logiciel** (software backplane) : regroupement de fonctionnalités d'enfichage d'outils logiciels qui fixe des règles d'homogénéité auxquelles doivent se conformer les outils enfichés.

0.2.45 **Fourniture** (deliverable - 0.2.45) : article ou ressource qui doit être mis à la disposition des évaluateurs pour l'évaluation.

0.2.46 **Impartialité** (impartiality - 0.2.51) : liberté par rapport à tout facteur pouvant biaiser un résultat.

0.2.47 **Manuel d'évaluation de la sécurité des technologies de l'information** (information technology security evaluation manual - 0.2.53) : document technique contenant suffisamment de détails sur les méthodes et les procédures d'évaluation pour permettre la reconnaissance mutuelle.

0.2.48 **Objectivité** (objectivity - 0.2.56) : propriété d'un test, pour obtenir le résultat, en faisant intervenir le moins possible de jugements subjectifs ou d'opinions.

0.2.49 **Objet** (object - 0.2.55) : entité passive qui contient ou qui reçoit de l'information.

0.2.50 **Organisme de certification** (certification body - 0.2.41) : organisation nationale, souvent l'autorité nationale en matière de sécurité, responsable de l'administration des évaluations menées selon les ITSEC dans ce pays.

0.2.51 **Programme de travail pour l'évaluation** (evaluation work programme - 0.2.48) : description de l'organisation du travail nécessaire à l'évaluation ; c'est-à-dire une description des lots engagés dans l'évaluation et des rapports existant entre ceux-ci.

0.2.52 **Raffinement correct** (correct refinement - 0.2.43) : un raffinement d'une fonction décrite à un certain niveau d'abstraction est dit correct si la totalité des effets décrits à un niveau d'abstraction inférieur correspond à tous les effets décrits au niveau d'abstraction supérieur.

0.2.53 **Rapport d'anomalie** (problem report - 0.2.59) : rapport concis, produit par les évaluateurs, envoyé à l'OC, décrivant une erreur, une vulnérabilité potentielle ou une vulnérabilité réelle de la cible d'évaluation.

0.2.54 **Rapport technique d'évaluation** (evaluation technical report - 0.2.47) : rapport produit par un CESTI et soumis à l'OC, détaillant les conclusions de l'évaluation et servant de base à la certification de la cible d'évaluation.

0.2.55 **Réévaluation** (re-evaluation - 0.2.60) : évaluation, suite à des changements, d'une cible d'évaluation ayant déjà fait l'objet d'une évaluation.

0.2.56 **Répétabilité** (repeatability - 0.2.62) : la répétition de l'évaluation de la même cible d'évaluation avec la même cible de sécurité évaluée par le même CESTI conduit au même verdict global que celui établi lors de la première évaluation (e.g. E0 ou E5).

0.2.57 **Représentation** (representation - 0.2.63) : spécification de la cible d'évaluation correspondant à une phase de son développement (à savoir : spécification des besoins, conception générale, conception détaillée et réalisation).

0.2.58 **Reproductibilité** (reproducibility - 0.2.64) : la répétition de l'évaluation de la même cible d'évaluation avec la même cible de sécurité évaluée par un autre CESTI conduit au même verdict global que celui établi lors de la première évaluation (e.g. E0 ou E5).

0.2.59 **Réutilisation** (re-use - 0.2.61) : utilisation de résultats précédents lorsqu'un ou plusieurs composants déjà évalués sont intégrés dans un système ou un produit.

0.2.60 **Schéma national** (national scheme - 0.2.54) : ensemble de règles et de lois nationales pour l'évaluation et la certification selon les ITSEC et l'ITSEM.

0.2.61 **Sujet** (subject - 0.2.65) : entité active, généralement une personne, un processus ou un dispositif [TCSEC].

0.2.62 **Trace d'audit** (audit trail - 0.2.37) : ensemble d'informations recueillies par une cible d'évaluation correspondant à des opérations imputables en vue de permettre un audit.

0.2.63 **Vulnérabilité potentielle** (potential vulnerability - 0.2.58) : vulnérabilité soupçonnée qui pourrait être utilisée pour compromettre un objectif de sécurité de la cible d'évaluation, mais dont l'exploitabilité ou l'existence n'a pas encore été démontrée.

0.2.64 **Vulnérabilité de construction** (construction vulnerability - 0.2.42) : vulnérabilités tirant profit d'une propriété de la cible d'évaluation introduite pendant sa construction.

0.2.65 **Vulnérabilité** (vulnerability - 0.2.67) : faiblesse dans la sécurité d'une cible d'évaluation (due par exemple à des erreurs d'analyse, de conception, de réalisation ou d'exploitation).

0.2.66 **Vulnérabilité en exploitation** (operational vulnerability - 0.2.57) : vulnérabilités tirant profit de faiblesses dans les contre-mesures non techniques d'une cible d'évaluation pour violer sa sécurité.

0.2.67 **Vulnérabilité exploitable** (exploitable vulnerability - 0.2.49) : vulnérabilité qui peut être exploitée dans la pratique pour compromettre un objectif de sécurité de la cible d'évaluation.

Références

0.2.68 Dans ce document, il est fait référence aux ouvrages suivants :

BDSS Risk Quantification Problems and Bayesian Decision Support System Solutions, Will Ozier, Information Age, Vol. 11, No. 4, October 1989.

BOE Characteristics of Software Quality - TRW North Holland, B.W. Boehm, Software Engineering Economics - Prentice Hall, 1975.

CESG2 Handbook of Security Evaluation, CESG Memorandum No. 2, Communications-Electronics Security Group, United Kingdom, November 1989.

CRAMM CCTA Risk Analysis and Management Methodology, Guidance on CRAMM for Management, Version 2.0, CCTA, February 1991.

DTI23 Evaluation and Certification Manual, V23 Department of Trade and Industry, United Kingdom, Version 3.0, February 1989.

ECMA A Reference Model for Frameworks of Computer-Assisted Software Engineering Environments, ECMA TR/55.

EN45 Critères généraux concernant le fonctionnement de laboratoires d'essais, EN 45001, AFNOR, Normes françaises, décembre 1989.

GASSER Building a Secure Computer System, Morrie Gasser, Van Nostrand Reinhold.

GISA1 IT Evaluation Manual, GISA 1990.

GISA2 IT Sicherheitshandbuch, BSI 7105, Version 1.0, March 1992.

GUI25 Prescriptions générales concernant la compétence des laboratoires d'étalonnage et d'essais, International Standards Organisation, ISO Guide 25, Réseau national d'essais, éd. 3, 1990.

ISO65A Software for Computers in the Application of Industrial Safety Related Systems, ISO/IEC JTC1/SC27 N381, November 1991.

ITSEC Critères d'Évaluation de la Sécurité des Systèmes Informatiques, critères harmonisés provisoires de la France, l'Allemagne, les Pays-Bas et du Royaume Uni, version 1.2, juin 1991.

LINDE Operating System Penetration, R Linde, Proceedings of the AFIPS, NCC, pp 361-368, 1975.

MCC Factors in Software Quality, J A McCall, General Electric n.77C1502, June 1977.

MS1629A Procedures for performing a failure mode, effects and criticality analysis, MIL-STD-1629A, US DoD, November 1980.

NIS35 Interpretation of Accreditation Requirements for IT Test Laboratories for Software and Communications Testing Services, NAMAS Information Sheet NIS35, NAMAS Executive, National Physics Laboratory, United Kingdom, November 1990.

OSI OSI Basic Reference Model, Part 2 - Security Architecture, ISO 7498 (1988(E)).

PCTE Portable Common Tool Environment Abstract Specification (December 1990; ECMA 149).

PCTE+ Portable Common Tool Environment (Extended) Definition Team Final Report (14 December 1992).

SRMM Shared Resource Matrix Methodology: An Approach to Identifying Storage and Timing Channels, R A Kemmerer, ACM Transactions on Computer Systems, Vol. 1, No. 3, August 1983.

TCSEC Trusted Computer Systems Evaluation Criteria, DoD 5200.28-STD, Department of Defense, United States of America, December 1985.

TNI Trusted Network Interpretation of the TCSEC, National Computer Security Center, United States of America, NCSC-TG-005, Version 1, 31 July 1987.

TDI Trusted Database Interpretation of the TCSEC, National Computer Security Center, United States of America, NCSC-TG-021, April 1991.

Partie 1 Cadre de la sécurité des TI

Table des matières

Figures

Chapitre 1.1 Introduction

Biens, menaces, risques, confiance et contre-mesures

1.1.1 Les Technologies de l'Information (TI) sont devenues essentielles pour la conduite efficace des entreprises ou des affaires des états et deviennent de plus en plus importantes pour les affaires des personnes privées concernées par l'utilisation des TI. L'information doit être acquise et protégée pour faire progresser les entreprises ou les affaires d'état et devrait donc être considérée comme un **bien**. L'importance de tels biens est généralement exprimée en termes de dommages consécutifs à la réalisation de menaces. Les dommages peuvent être la conséquence directe ou indirecte de la divulgation, la modification illicite, la destruction ou le détournement des informations. Le risque augmente avec l'importance des dommages éventuels et la probabilité de la réalisation des menaces.

1.1.2 Les informations des systèmes TI doivent être protégées contre les menaces qui peuvent induire des conséquences néfastes pour les biens. Les menaces peuvent être délibérées (par exemple : des attaques) ou involontaires (par exemple : des erreurs ou des défaillances).

1.1.3 Afin de réduire les risques, des **contre-mesures** spécifiques seront choisies. Ces contre-mesures seront par nature physiques, liées au personnel, organisationnelles ou techniques. Les *contre-mesures techniques*, ou *contre-mesures TI*, sont les fonctions et mécanismes dédiés à la sécurité du système TI ; les *contre-mesures non techniques*, ou *contre-mesures non TI*, sont les contre-mesures physiques, liées au personnel et organisationnelles. L'évaluation ITSEC porte principalement sur les contre-mesures techniques.

1.1.4 Le premier objectif de sécurité d'un système TI est de réduire, à un niveau acceptable pour l'organisation concernée, les risques associés. Cet objectif peut être atteint via les fonctions de sécurité et les caractéristiques (intrinsèques) du système TI.

1.1.5 La confiance qui peut être accordée à la sécurité fournie par un système TI est appelée assurance. Plus grande est l'assurance, plus grande est la confiance en la protection par le système des biens contre la menace, avec un niveau acceptable de risques résiduels.

1.1.6 Plus le niveau d'évaluation ITSEC et la résistance des mécanismes sont élevés, plus l'assurance que l'utilisateur peut avoir dans les contre-mesures introduites dans le système ou le produit TI est importante. Le niveau d'évaluation exigé par un utilisateur est fonction du niveau acceptable de risques résiduels identifiés et ne peut être déterminé qu'à l'aide d'une analyse des risques et des menaces qui s'appliquent à un cas particulier. Il faut parvenir à un équilibre entre la sécurité et les coûts. Les produits ou systèmes avec des niveaux d'évaluation élevés sont généralement plus onéreux, car les coûts de développement et d'évaluation ont tendance à augmenter avec le niveau d'évaluation. Des conseils pour déterminer un niveau d'évaluation en fonction de paramètres de l'environnement sont fournis, par exemple, dans [GISA2]. Des avis spécifiques peuvent être demandés aux organisations nationales mentionnées dans la partie 2 de l'ITSEM.

Processus s'inscrivant dans le cadre de la sécurité des TI

1.1.7 Divers processus contribuent à l'objectif de la sécurité des TI. Ceux-ci sont illustrés dans la figure 1.1.1.

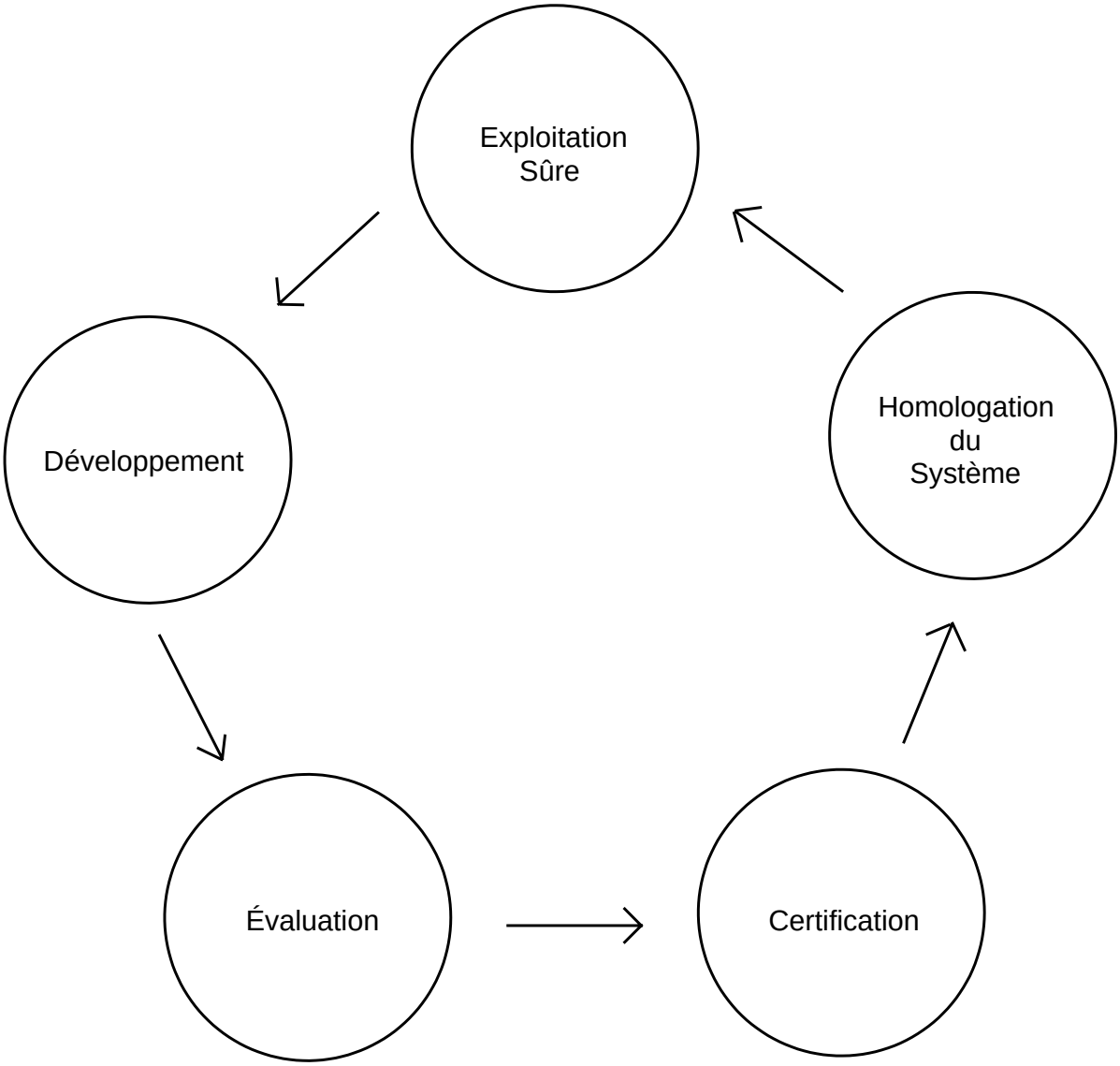


Figure 1.1.1 Processus s'inscrivant dans le cadre de la sécurité des TI

1.1.8 Cette figure présente le contexte idéal dans lequel s'inscrivent l'évaluation et la certification de la sécurité des TI. Les flèches indiquent qu'un processus fournit les données pour le traitement suivant. Les processus peuvent s'entrelacer partiellement. L'enchaînement des traitements est le plus souvent cyclique et itératif.

1.1.9 Au cours du processus de développement, un système ou un produit TI est construit. Au cours du processus d'évaluation, le système ou le produit est examiné sur des critères bien définis d'évaluation de la sécurité. Au cours du processus de certification, la validité des résultats de l'évaluation et l'application correcte des critères d'évaluation sont confirmées. Le processus d'homologation de système permet de confirmer que l'utilisation d'un système TI est acceptable dans un environnement particulier et dans un but particulier. Dans le processus d'exploitation sûr, un système homologué est exploité conformément à des procédures agréées, mais des changements apportés à l'environnement peuvent entraîner des besoins de modifications du système qui se répercutent sur le processus de développement.

1.1.10 Les termes homologation et accréditation[1] permettent de distinguer deux contextes différents. L'accréditation d'un centre d'évaluation de la sécurité des technologies de l'information (CESTI) est la procédure pour reconnaître à la fois son **impartialité** et ses compétences techniques pour conduire des évaluations. L'homologation d'un système TI (telle que définie dans l'introduction des ITSEC) est une procédure de réception d'un système TI qui doit être utilisé dans un environnement particulier. L'homologation d'un système porte à la fois sur les contre-mesures TI et non TI, tandis que l'ITSEM traite principalement des contre-mesures TI. L'homologation de systèmes est hors du champ d'application des ITSEC et de l'ITSEM.

Contexte des évaluations

1.1.11 Le contexte des évaluations présente trois aspects :

a) les critères ;

b) le cadre méthodologique ;

c) **les schémas nationaux**.

1.1.12 Les critères représentent le barème avec lequel la sécurité d'un produit ou d'un système TI peut être mesurée pour son évaluation, son développement et son acquisition. Les critères définissent ce qui doit être évalué. Le cadre méthodologique indique comment l'évaluation devrait être effectuée sur la base des critères. Les schémas nationaux fournissent les règles d'organisation qui s'appliquent aux processus d'évaluation, de certification et d'accréditation de laboratoires en termes de rôles, de procédures, de droits et d'obligations. Les critères sont contenus dans les ITSEC et la méthodologie associée est donnée dans l'ITSEM, développée à un niveau de détail qui suffit pour faciliter une reconnaissance mutuelle entre les schémas nationaux. Les questions relatives aux schémas nationaux sont traitées dans la partie 2 de l'ITSEM ainsi que dans la documentation afférente au schéma établie par chaque pays.

1. NdT: les termes homologation et accréditation correspondent au seul terme anglais "accreditation"

Chapitre 1.2 Processus d'évaluation et de certification

Concepts de base

1.2.1 Le processus d'évaluation, décrit dans ses grandes lignes dans le présent chapitre, constitue un cadre qui décrit les aspects organisationnels et procéduraux de la conduite d'une évaluation. Il existe de nombreux sujets connexes à une évaluation, qui sont traités différemment d'un pays à l'autre par exemple pour des raisons de droit ou de sécurité nationale. Ce sont les règles du schéma national qui prévalent dans chaque pays. Les sujets relatifs aux schémas nationaux sont traités dans la partie 2 de l'ITSEM.

1.2.2 Lorsqu'elles sont effectuées dans le cadre d'activités commerciales, les évaluations selon les ITSEC sont soumises aux conditions économiques du marché des TI. Elles doivent être commercialement réalisables, c'est-à-dire d'un coût abordable, et être opportunes. Cet objectif doit être mesuré aux bénéfices de l'évaluation. Les principes qui régissent le processus d'évaluation et de certification sont présentés dans la partie 3 de l'ITSEM.

1.2.3 Dans ce type d'évaluation :

a) les commanditaires peuvent établir les objectifs du processus d'évaluation ;

b) des ressources du CESTI peuvent être mises à la disposition du commanditaire à sa demande ;

c) la maintenance des **certificats** et **rapports de certification** au moyen d'une **réévaluation** est facilement réalisable.

Parties impliquées

1.2.4 Les parties suivantes sont directement impliquées dans le processus d'évaluation :

a) le commanditaire de l'évaluation ;

b) les développeurs du produit ou du système TI ;

c) le centre d'évaluation de la sécurité des technologies de l'information (CESTI) ;

d) l**'organisme de certification** (OC).

1.2.5 Les autres parties concernées par l'évaluation et la certification sont les utilisateurs et les responsables de l'homologation du système. Ils sont principalement concernés par l'acquisition et l'exploitation sûre.

1.2.6 La figure 1.2.1 montre que toutes les parties impliquées considèrent l'évaluation et la certification selon un angle différent en fonction de leurs rôles.

1.2.7 L'ITSEM contient des descriptions ainsi que des conseils à l'attention des commanditaires, des développeurs, des CESTI, des responsables de l'homologation de systèmes et des organismes de certification. En outre, des obligations sont faites aux évaluateurs dans la partie 4 de l'ITSEM.

1.2.8 Le commanditaire d'une évaluation est la partie qui lance et finance l'évaluation. Dans le cas de l'évaluation d'un système, il est vraisemblable que le commanditaire et le responsable de l'homologation de systèmes constitueront la même organisation.

1.2.9 Le CESTI mène l'évaluation, habituellement comme une activité commerciale. L'évaluation, conformément aux ITSEM et ITSEC, comprend un examen approfondi d'une cible d'évaluation pour rechercher des **vulnérabilités** et déterminer dans quelle mesure la cible de sécurité de la cible d'évaluation est satisfaite par sa réalisation.

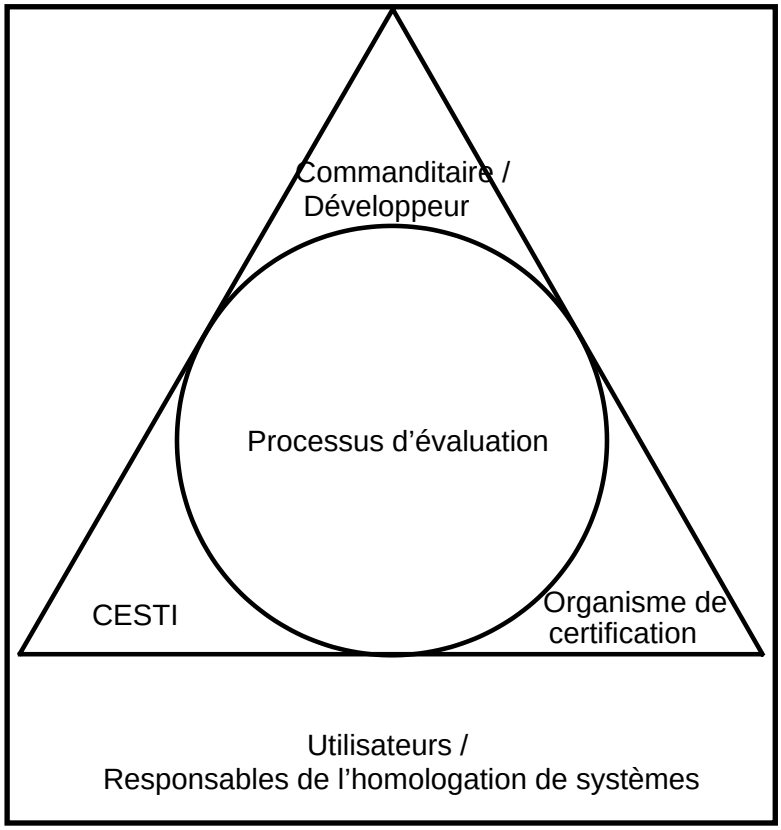


Figure 1.2.1 Parties impliquées dans, ou concernées par, l'évaluation et la certification

1.2.10 L'indépendance du CESTI par rapport à toute pression d'origine commerciale ou tout autre qui émanerait du commanditaire ou du développeur d'une cible d'évaluation est considérée comme un facteur clé. Cela n'écarte pas pour autant une évaluation par soi-même ou évaluation "primaire", dans le sens d'une évaluation menée par une autre partie de l'organisation du commanditaire ou du développeur, pourvu que les exigences du schéma national soient satisfaites.

1.2.11 Il est probable que les travaux d'évaluation soient effectués sous couvert d'un accord de confidentialité établi avec le commanditaire ou le développeur. Un CESTI devrait garantir la confidentialité commerciale.

1.2.12 L'impartialité du CESTI en ce qui concerne les évaluations effectuées est également un facteur important. Les schémas nationaux peuvent imposer des exigences auxquelles doit satisfaire un CESTI.

1.2.13 L'organisme de certification (OC) contrôle la validité des résultats d'une évaluation et vérifie que les critères d'évaluation ont été correctement appliqués. Cette mesure vise à garantir l'uniformité et la conformité des procédures d'évaluation à l'ITSEM et aux ITSEC, ainsi que la cohérence et la compatibilité des résultats d'évaluation. L'OC prépare et délivre le certificat et le rapport de certification pour les cibles d'évaluation dont on a trouvé qu'elles satisfont à leur cible de sécurité et, par là même, aux exigences du Chapitre 5 des ITSEC.

1.2.14 Le certificat/rapport de certification sera publié. La partie 2 de l'ITSEM fournit des renseignements quant à leur format et leur contenu.

Phases du processus d'évaluation

1.2.15 Le processus d'évaluation est divisé en trois phases :

a) Phase I Préparation ;

b) Phase II Conduite ;

c) Phase III Conclusion.

1.2.16 Le processus est décrit ici dans ses grandes lignes pour une évaluation type. Dans la pratique, il existe un certain nombre d'options, notamment lorsque l'évaluation est effectuée simultanément au processus de développement. Les trois phases sont décrites plus en détail dans la partie 4 de l'ITSEM.

1.2.17 La phase I comprend le premier contact entre le commanditaire et un CESTI, toute étude de faisabilité et la préparation à l'évaluation. L'étude de faisabilité est facultative, mais particulièrement conseillée aux commanditaires et développeurs qui ne bénéficient pas d'une expérience préalable en évaluation. Cette étude de faisabilité confirmera que le commanditaire et le développeur sont bien préparés à la conduite d'une évaluation et impliquera au moins une revue de la cible de sécurité. Lorsque la réussite de l'évaluation semble plausible, on établit une liste des **fournitures** exigées pour l'évaluation, un plan pour leur livraison et un **programme de travail pour l'évaluation**. Il est raisonnable de prendre contact avec l'OC de façon à établir un calendrier qui a l'accord du commanditaire, du développeur, du CESTI et de l'OC.

1.2.18 Un contrat entre le commanditaire et le CESTI est normalement signé au cours de la phase I. Ce contrat prend en considération la législation nationale et comprend généralement un accord de confidentialité.

1.2.19 Le programme de travail pour l'évaluation d'une cible d'évaluation particulière est fondé sur les fournitures, leur calendrier de livraison et les critères des ITSEC. Le travail demandé est réparti selon des activités d'évaluation à mener par les évaluateurs suivant un calendrier prévu. Le développement du programme de travail pour l'évaluation s'apparente à l'élaboration du plan de développement dans le cycle de vie d'un développement logiciel. Il n'est pas prescrit dans les ITSEC d'appliquer les critères selon un ordre déterminé, mais certains enchaînements d'activités sont plus raisonnables et plus efficaces que d'autres. La partie 4 de l'ITSEM fournit des renseignements à ce sujet.

1.2.20 La phase II est la partie principale du processus d'évaluation. Les évaluateurs effectuent les tâches d'évaluation des critères ITSEC. Ces tâches comprennent des tests de pénétration fondés sur la liste des **vulnérabilités potentielles** et d'autres tests. Le **Rapport technique d'évaluation** (RTE) est préparé au cours de cette phase.

1.2.21 Dans la phase III, le CESTI fournira le résultat final du processus d'évaluation, à savoir le RTE, au commanditaire/développeur et à l'OC, comme une donnée de base du processus de certification. Des contraintes de confidentialité peuvent exiger une gestion différente. Comme le RTE contient des données sensibles, il n'est pas un document public et il est soumis aux règles du schéma national. Le CESTI peut être amené à fournir une assistance technique à l'OC concernant le RTE.

1.2.22 La certification est décrite dans ses grandes lignes dans la partie 2 de l'ITSEM.

Traitement des problèmes

1.2.23 Les problèmes identifiés par le CESTI au cours d'une évaluation sont généralement débattus entre le commanditaire, le développeur et le CESTI. Dans le cas de problèmes sérieux, il faudrait demander un avis à l'OC. Si les problèmes ne peuvent être résolus, le commanditaire peut décider de renoncer à l'évaluation. Les règles du schéma national prévalent dans tous les cas.

Évaluations simultanées et consécutives

1.2.24 Une évaluation peut être effectuée après que le développement d'une cible d'évaluation a été achevé, c'est une *évaluation consécutive*, ou parallèlement au développement d'une cible d'évaluation, c'est une *évaluation simultanée*.

1.2.25 La principale différence entre les évaluations simultanées et consécutives réside dans la disponibilité des diverses **représentations** de la cible d'évaluation en tant que fournitures. Dans le cas d'une évaluation consécutive, l'ensemble des fournitures exigées par les ITSEC, de la cible de sécurité à la cible d'évaluation opérationnelle, est normalement disponible dès le début de l'évaluation. Dans le cas d'une évaluation simultanée, les fournitures seront délivrées par le commanditaire/développeur au fur et à mesure de l'avancement du développement. Les évaluations simultanées donnent la possibilité au commanditaire/développeur de réagir rapidement face aux problèmes rencontrés.

1.2.26 La différence qui existe entre les deux types d'évaluation n'a aucune répercussion technique, mais a une influence sur l'organisation d'une évaluation, c'est-à-dire sur le programme de travail pour l'évaluation. Dans le cadre d'une évaluation simultanée, l'ordre et les délais des activités d'évaluation sont orientés vers la livraison des fournitures. Les tests de pénétration et les autres tests ne peuvent être effectués avant que la cible d'évaluation opérationnelle ne soit disponible. Les conséquences possibles des retards et des itérations sont à prendre en compte.

Evaluations de systèmes et de produits

1.2.27 Selon les ITSEC, un produit est un *paquetage logiciel et/ou matériel TI qui assure une fonctionnalité conçue pour être utilisée ou incorporée au sein de multiples systèmes* et un système est *une installation spécifique de TI avec un but et un environnement d'exploitation particuliers.*

1.2.28 Les évaluations d'un produit et d'un système sont semblables ; les deux peuvent être simultanées ou consécutives. La principale différence concerne la cible de sécurité. Dans le cas d'un système, l'environnement est identifié et les menaces ou les objectifs de sécurité sont réels et peuvent être spécifiés dans le détail. Dans le cas d'un produit, les menaces ou les objectifs de sécurité doivent être estimés en anticipant l'objectif opérationnel et l'environnement du produit, et ne peuvent être exprimés qu'en termes génériques.

Réévaluation et réutilisation de résultats d'évaluation

1.2.29 Lorsqu'un produit ou un système est évalué et certifié, le certificat/rapport de certification s'applique uniquement à la version et à la configuration évaluées. Il est vraisemblable que les exigences de sécurité et les produits ou systèmes évalués seront sujet à modification. Le certificat et rapport de certification peut ne pas s'appliquer à un système ou produit modifié et une réévaluation peut alors être exigée. De plus amples renseignements sont donnés à l'annexe 6.D de la partie 6.

1.2.30 Au cours du processus de réévaluation, il peut être souhaitable de **réutiliser** les résultats de l'évaluation précédente de la cible d'évaluation. Ce point est traité dans le chapitre 4.6 de la partie 4 et dans l'annexe 6.F de la partie 6.

Partie 2 Schémas de certification

Table des matières

Chapitre 2.1 Introduction

2.1.1 La version 1.2 des ITSEC établit, au paragraphe 1.31 qui décrit le processus de certification :

Pour que les présents critères aient une valeur pratique, ils devront s'appuyer sur des organisations pratiques permettant d'assurer la mise en place et le contrôle d'une évaluation indépendante, pilotées par des ***organismes de certification*** *convenablement qualifiés et reconnus au plan national. Ces organismes délivreront des certificats confirmant la cotation de la sécurité des TOE, telle que déterminée par des évaluations indépendantes convenablement conduites.*

2.1.2 Ces schémas d'organisation veillent à ce que la méthodologie exposée dans l'ITSEM soit appliquée de façon cohérente et correcte au cours de l'évaluation des cibles d'évaluation selon les critères ITSEC ; ils constituent en cela un préalable nécessaire à une reconnaissance mutuelle internationale des certificats délivrés par leurs organismes de certification.

2.1.3 Sous réserve que tous les schémas assurent la conformité des évaluations par rapport à l'ITSEM en ce qui concerne l'exécution des tâches d'évaluation décrites dans les ITSEC, il devrait être possible d'admettre que le résultat d'une évaluation conduite dans le cadre d'un schéma spécifique soit identique à celui qui serait obtenu dans le cadre de tout autre schéma.

Chapitre 2.2 Normes

2.2.1 Les normes internationales et européennes (ISO Guide 25 [GUI25] et EN45001 [EN45]) ont été établies pour fournir des indications générales en matière d'accréditation et de fonctionnement des laboratoires d'essais. Ces normes définissent un cadre pour le test objectif de tous les types de produits, et non pas seulement ceux qui relèvent du domaine des TI. Lorsqu'il s'agit de l'évaluation et de la certification de la sécurité des TI, il peut être utile que ces normes soient respectées en vue de faciliter l'acceptation de tout accord de reconnaissance mutuelle par la Commission Européenne pour la Certification et les Essais des TI (ECITC).

2.2.2 Cependant, il reste que certains facteurs inhérents à la sécurité des TI peuvent rendre indésirable, ou difficilement réalisable, la conformité à ces normes. Par conséquent, des interprétations de la norme EN45001pour l'évaluation de la sécurité des TI sont élaborées dans divers pays pour être intégrées aux règlements nationaux en matière d'évaluation, de certification et d'accréditation et d'agrément de centres d'évaluation, tout en respectant l'esprit de ces normes. Même en disposant de ces interprétations établies, il reste certains aspects de l'évaluation de la sécurité des TI qui doivent être contrôlés par un organisme de certification de manière à assurer des résultats d'évaluation comparables.

Chapitre 2.3 Mise en place des CESTI

2.3.1 Il est essentiel que les évaluations soient conduites par des centres d'évaluation expérimentés dans les domaines de la sécurité des TI et du cadre méthodologique des ITSEC et des ITSEM. Ces centres devraient donc chercher à être conformes aux exigences de la norme EN45001 et à leur interprétation propre à la sécurité des TI. Cependant, une demande formelle d'accréditation selon cette norme n'est pas obligatoire. Cela a conduit certains pays à élaborer des schémas pour l'agrément des CESTI en ajoutant des exigences, en particulier sur des aspects liés à la sécurité des TI, à l'accréditation fondée sur la norme EN45001. Ces exigences supplémentaires ne sont pas du ressort de l'ITSEM et ne sont pas davantage développées ici. Cependant, soit ces aspects ne sont pas pertinents d'une reconnaissance mutuelle, soit ils feraient sûrement explicitement partie de tout accord de reconnaissance mutuelle.

2.3.2 Certains schémas nationaux d'agrément ou d'accréditation sont déjà mis en place et sont soumis aux exigences mentionnées ci-dessus. Les centres qui sont intéressés par de plus amples renseignements, notamment sur ces exigences supplémentaires, doivent demander l'avis de l'organisme national approprié (voir le chapitre 2.7).

Chapitre 2.4 Évaluation et certification : objectifs et avantages

2.4.1 L'objectif principal de la certification est de fournir une confirmation indépendante qui atteste que les évaluations ont été correctement effectuées, conformément aux critères, méthodes et procédures approuvés et que les conclusions de l'évaluation sont cohérentes avec les faits présentés. Dans le cadre d'un schéma contrôlé par un organisme de certification unique, ceci permet en retour de motiver la confiance dans le fait que différents centres d'évaluation qui participent au même schéma se conforment aux mêmes normes et que les conclusions de deux quelconques de ces centres d'évaluations sont également fiables. Les principaux aspects qui motivent cette confiance se résument en quatre principes :

a) **l'impartialité :** les évaluations doivent être libres de tout facteur pouvant les biaiser.

b) **L'objectivité :** la propriété d'un test, pour obtenir le résultat, en faisant intervenir le moins possible de jugements subjectifs ou d'opinions.

c) **La répétabilité :** la répétition de l'évaluation de la même cible d'évaluation avec la même cible de sécurité par le même CESTI conduit au même verdict global que celui qui a été établi lors de la première évaluation.

d) **La reproductibilité :** la répétition de l'évaluation de la même cible d'évaluation avec la même cible de sécurité par un autre CESTI conduit au même verdict global que celui qui a été établi par le premier CESTI.

2.4.2 Les divers partenaires impliqués peuvent tirer plusieurs avantages du processus d'évaluation et de certification. Quelques uns sont mentionnés ci-dessous :

a) les fournisseurs/développeurs/commanditaires tirent avantage de l'évaluation et de la certification car :

- les clients sont avertis qu'une évaluation réussie effectuée par un tiers indépendant a accordé les capacités annoncées au produit ;
- un certificat approprié permet d'accéder aux marchés spécialisés et de s'y faire accepter ;
- les produits certifiés peuvent être exploités comme des composants de base pour des systèmes certifiés ;
- la certification fournit également une déclaration de la qualité d'un produit ou d'un système et de son développement ;

b) les utilisateurs/responsables de l'homologation de systèmes tirent avantage de l'évaluation et de la certification car :

- ils peuvent être sûrs que l'examen par un tiers a confirmé les annonces de sécurité d'un fournisseur ;

- un certificat constitue une base intéressante de comparaison entre différents produits ;

- ils bénéficient de conseils pour garantir que la configuration sûre d'une cible d'évaluation certifiée n'est pas compromise ;

c) les évaluateurs tirent avantage de l'évaluation et de la certification car :

- ils disposent d'une clientèle potentielle plus large ;

- le contrôle indépendant exercé par l'organisme de certification fournit des conseils aux évaluateurs pour assurer qu'ils remplissent leurs obligations ;

d) les schémas de certification en tirent avantage car ils permettent :

- d'effectuer la comparaison, le développement et la maintenance de normes internationales ;

- de mesurer les normes internes par rapport à un ensemble de critères internationaux ;

- d'encourager les commanditaires en ouvrant des marchés plus vastes à leurs produits.

Chapitre 2.5 Le schéma de certification

2.5.1 Les objectifs principaux d'un organisme de certification sont, en premier lieu, de créer les conditions qui permettent que les travaux de tous les CESTI réalisés dans le cadre d'un schéma soient exacts et cohérents et que leurs conclusions soient valides, répétables et reproductibles ; le second objectif est de fournir, dans le cas d'évaluations spécifiques, une confirmation indépendante que les évaluations ont été conduites conformément aux critères, méthodes et procédures agréés. Pour atteindre ces objectifs, l'organisme de certification doit accomplir les fonctions suivantes (entre autres) :

a) autoriser la participation des CESTI au schéma, en assurant la conformité avec les exigences du schéma considéré ;

b) surveiller ce que font les CESTI et comment ils respectent et appliquent les ITSEC et l'ITSEM, en donnant, si besoin est, des conseils supplémentaires ;

c) surveiller toute évaluation effectuée par un CESTI ;

d) passer en revue tous les rapports d'évaluation de manière à estimer les conséquences de leurs résultats pour la sécurité et à assurer leur conformité par rapport aux critères ITSEC et à l'ITSEM ;

e) produire des rapports de certification ;

f) publier des certificats et des rapports de certification.

2.5.2 L'ensemble de ces activités est effectué dans le cadre d'un schéma de certification. La cohérence très importante des normes (et donc de la validité et de la fiabilité des résultats) entre les différents CESTI ne peut être atteinte que dans le cadre d'un tel schéma. La cohérence est importante non seulement pour le client et pour la confiance qu'il peut accorder à une évaluation (et par là même au produit ou système évalué), mais aussi parce qu'il s'agit d'une condition préalable pour atteindre une reconnaissance mutuelle internationale.

2.5.3 Les fonctions d'un schéma de certification sont, entre autres : la définition des types de produits et systèmes qui peuvent être évalués, l'émission des certificats et des rapports de certification ainsi que leur maintenance ultérieure (y compris la prévention d'emploi abusif), la publication de documents relatifs au schéma et à son fonctionnement, et d'autres aspects liés à l'administration au jour le jour du schéma.

2.5.4 Toute exigence nationale spécifique imposée dans certains schémas particuliers ne relèvent pas de l'ITSEM. Ceux qui cherchent de plus amples renseignements sur les **schémas nationaux** particuliers, doivent demander l'avis de l'organisme approprié parmi ceux mentionnés au chapitre 2.7.

Chapitre 2.6 Contenu des certificats/rapports de certification

2.6.1 Les certificats et rapports de certification seront accessibles au public.

2.6.2 Les certificats et rapports de certification devraient contenir au moins :

a) **Introduction** :

- un texte liminaire défini par le schéma national ;

b) **Sommaire** :

- l'identité du centre d'évaluation de la sécurité des technologies de l'information (CESTI) ;
- l'identification de la cible d'évaluation (TOE) y compris le numéro d'exemplaire et le numéro d'édition ;
- l'identification de l'évaluation attribuée par l'organisme de certification ;
- un résumé des principales conclusions de l'évaluation ;
- l'identité du développeur (y compris celle des sous-traitants, le cas échéant) ;
- l'identité du commanditaire ;
- le niveau réel atteint par l'évaluation ;

c) **Présentation du produit** :

- une description des configurations évaluées ;
- une description des matériels ;
- une description des microprogrammes ;
- une description des logiciels ;
- une description de la documentation ;

d) **L'évaluation** :

- une brève description de la cible de sécurité, qui intégre une description des caractéristiques de sécurité de la cible d'évaluation ;
- une référence au **Rapport technique d'évaluation** ;

- l'identité du centre d'évaluation de la sécurité des technologies de l'information ;

- un résumé des principales conclusions de l'évaluation ;

e) **Certification**

- la portée du certificat (par exemple : toute limite pour la mise en œuvre de la cible d'évaluation).

Chapitre 2.7 Liste des contacts

2.7.1 Une liste des contacts susceptibles de fournir des avis sur l'évaluation et la certification est donnée ci-après :

Pour la France :

Service Central de la Sécurité des Systèmes d'Information
18 rue du Docteur Zamenhof
F-92131 ISSY LES MOULINEAUX

Pour l'Allemagne :

Organisme d'accréditation :

Bundesamt für Sicherheit in der Informationstechnik
Referat II 4
Postfach 20 03 63
D-53133 BONN

Organisme de certification :

Bundesamt für Sicherheit in der Informationstechnik
Referat II 3
Postfach 20 03 63
D-53133 BONN

Pour les Pays-Bas :

National Security Service
P.O. Box 20010
NL-2500 EA THE HAGUE

Netherlands National Comsec Agency
Bezuidenhoutseweg 67
P.O. Box 20061
NL-2500 EB THE HAGUE

Pour le Royaume Uni :

Head of the Certification Body
UK IT Security Evaluation and Certification Scheme
Certification Body
PO Box 152
CHELTENHAM
Glos GL52 5UF

Page laissée blanche.

Partie 3 Philosophie, concepts et principes

Table des matières

Figures

Chapitre 3.1 Introduction

3.1.1 Cette partie décrit la philosophie de l'évaluation qui sous-tend les ITSEC et introduit les principes de base des travaux d'évaluation. Les concepts et notions utilisés dans le processus d'évaluation sont présentés. Cette partie fournit en outre les bases techniques pour les schémas nationaux d'évaluation et de certification (partie 2 de l'ITSEM) ainsi que pour le processus d'évaluation (partie 4 de l'ITSEM). Les principes seront traités dans le détail et mis en œuvre dans la partie 4 de l'ITSEM.

Chapitre 3.2 Philosophie générale de l'évaluation

Confiance et assurance

3.2.1 L'objectif principal de l'évaluation est d'acquérir la confiance dans le fait que la cible d'évaluation satisfait sa cible de sécurité. L'évaluation offre un degré donné de confiance attestant qu'il n'existe pas de **vulnérabilités exploitables**. Les avantages procurés par les objectifs de sécurité de la cible de sécurité ne sont pas mesurés au cours de l'évaluation car ceux-ci dépendent de l'application particulière qui est faite de la cible d'évaluation.

3.2.2 Le degré de confiance qui résulte d'une évaluation dépend du niveau de l'évaluation et de la résistance des mécanismes. Plus le niveau d'évaluation est élevé, plus la quantité d'informations pertinentes fournies et utilisées est importante, plus l'effort nécessaire pour l'évaluation est intense et plus l'assurance qui en résulte est grande. Ainsi, il convient de considérer l'évaluation comme une mesure unique mais complexe, effectuée avec un degré de précision qui est caractérisé par le niveau d'évaluation. En conséquence, plus il serait nécessaire de recourir à des **contre-mesures** fournies par une cible d'évaluation (pour, par exemple, ramener un risque important à un niveau acceptable), plus le niveau d'évaluation et la résistance des mécanismes devraient être élevés. Il existe une probabilité d'autant plus grande que la cible d'évaluation ait le comportement prévu et contre de façon adéquate les menaces.

3.2.3 L'assurance dans la sécurité fournie par un produit ou un système se déduit de l'examen du produit ou du système ainsi que de celui de ses **représentations**, et par la compréhension du processus suivant lequel il a été développé.

3.2.4 La plus grande contribution à l'assurance se déduit surtout de l'examen des représentations du produit ou du système lui-même. Un développeur certifié conformément à une norme de qualité telle l'ISO 9001 est vraisemblablement capable de produire des représentations adéquates. Néanmoins, en aucun cas, cette certification ne peut se substituer à une partie quelconque de l'évaluation.

Répétabilité, reproductibilité, impartialité et objectivité

3.2.5 Dans le cadre de l'évaluation et de la certification de la sécurité des TI, de même que dans le domaine de la science et du test, ***la répétabilité, la reproductibilité***, ***l'impartialité et l'objectivité*** sont considérées comme des principes importants.

3.2.6 Une évaluation est dite reproductible si la répétition de l'évaluation de la même cible d'évaluation, avec la même cible de sécurité par le même CESTI, produit le même verdict global que celui qui a été établi lors de la première évaluation.

3.2.7 Un résultat d'évaluation est dit répétable si la répétition de l'évaluation de la même cible d'évaluation, avec la même cible de sécurité, par un CESTI différent produit le même verdict global que celui qui a été établi par le premier CESTI.

3.2.8 Une évaluation est effectuée de manière impartiale si elle n'est pas biaisée pour obtenir un résultat particulier.

3.2.9 Une évaluation est effectuée de manière objective si le résultat est fondé sur des faits réels non déformés par les opinions ou les sentiments de l'évaluateur.

3.2.10 Un organisme de certification fait respecter ces quatre principes dans un schéma national. L'organisme de certification doit, en particulier, veiller à ce que la répétabilité et la reproductibilité des résultats de tests soient étendues au verdict global de l'évaluation.

Compréhension

3.2.11 Les critères d'évaluation décrivent les éléments de preuve que doit fournir un commanditaire/développeur d'évaluation, et ils décrivent aussi les points que les évaluateurs doivent vérifier. L'évaluation est fondée sur les informations fournies par le commanditaire et le développeur. L'assurance obtenu à la suite d'une évaluation est fonction des connaissances sur la cible d'évaluation (TOE) et son comportement. Il est d'autant plus facile de comprendre la cible d'évaluation que les informations qui la concerne sont pertinentes et complètes. Cela permet d'accroître la confiance que la cible d'évaluation satisfait à sa cible de sécurité. Ces faits se traduisent dans les exigences des ITSEC selon lesquelles les commanditaires/développeurs doivent produire les **fournitures** liées à la phase de construction sous la forme d'un ensemble de spécifications de la cible d'évaluation à différents niveaux d'abstraction.

3.2.12 L'évaluation associe observation, théorie et expérimentation. Un bon travail d'évaluation passe d'abord par la compréhension de la cible d'évaluation. La compréhension est obtenue par l'estimation de la cible de sécurité et des autres fournitures par rapport aux critères de conformité. Sur la base de leur compréhension de la cible d'évaluation et de sa cible de sécurité, les évaluateurs peuvent étudier la cible d'évaluation par rapport aux critères d'efficacité, à savoir si la cible d'évaluation peut agir de manière contraire aux spécifications de la cible de sécurité ou si elle est vulnérable aux menaces prévues.

3.2.13 Généralement, les cibles d'évaluations sont bien trop complexes pour que des tests suffisent à démontrer qu'elles satisfont leur cible de sécurité. Un jeu de tests exhaustif n'est pas réalisable. Par conséquent, la confiance en l'évaluation résulte de la compréhension de la cible d'évaluation par les évaluateurs au moyen de l'analyse de la documentation afférente à sa construction, son exploitation et au moyen de tests. Il subsistera toujours un doute en ce qui concerne la conformité de la cible d'évaluation à sa cible de sécurité. Il est impossible d'atteindre une assurance totale mais seulement la preuve d'une probabilité accrue que la cible d'évaluation satisfait à ses spécifications de sécurité. En règle générale, il est préférable de réduire les incertitudes résiduelles. Les évaluateurs doivent d'autant mieux comprendre la cible d'évaluation que le niveau d'évaluation est élevé.

Décomposition modulaire et principes du génie logiciel

3.2.14 La décomposition modulaire et les autres principes du génie logiciel tels que le masquage d'information, etc., fournissent généralement un bon point de départ pour faciliter et limiter les travaux d'évaluation nécessaires. De tels principes contribuent à identifier les **vulnérabilités potentielles**. Un développement bien documenté qui utilise des notations bien définies simplifie la compréhension de la cible d'évaluation par l'évaluateur. Les langages de programmation qui ont une syntaxe et une sémantique bien définies en sont un exemple concernant la phase de réalisation. Un développement fondé sur une bonne pratique du génie logiciel facilitera la tâche de l'évaluateur.

Processus d'évaluation

3.2.15 Il faudrait employer une méthode d'évaluation clairement comprise par toutes les parties. Les processus d'évaluation spécifiques pour des cibles d'évaluation particulières sont développés sur la base des critères ITSEC, des principes et de la philosophie d'évaluation, du **schéma national** et du processus d'évaluation décrit dans la partie 4 de l'ITSEM (voir figure 3.2.1). Le processus d'évaluation doit être normalisé pour rendre plus simple et plus efficace le contrôle et la comparaison des résultats. Dans la pratique, la méthode d'évaluation est mise en oeuvre par un **programme de travail pour l'évaluation** et par la prestation des activités identifiées de l'évaluateur. L'immense variété des cibles de sécurité et cibles d'évaluation possibles exclut des obligations détaillées. L'élaboration de la méthode d'évaluation est décrite dans la partie 4 de l'ITSEM ainsi que dans les schémas nationaux.

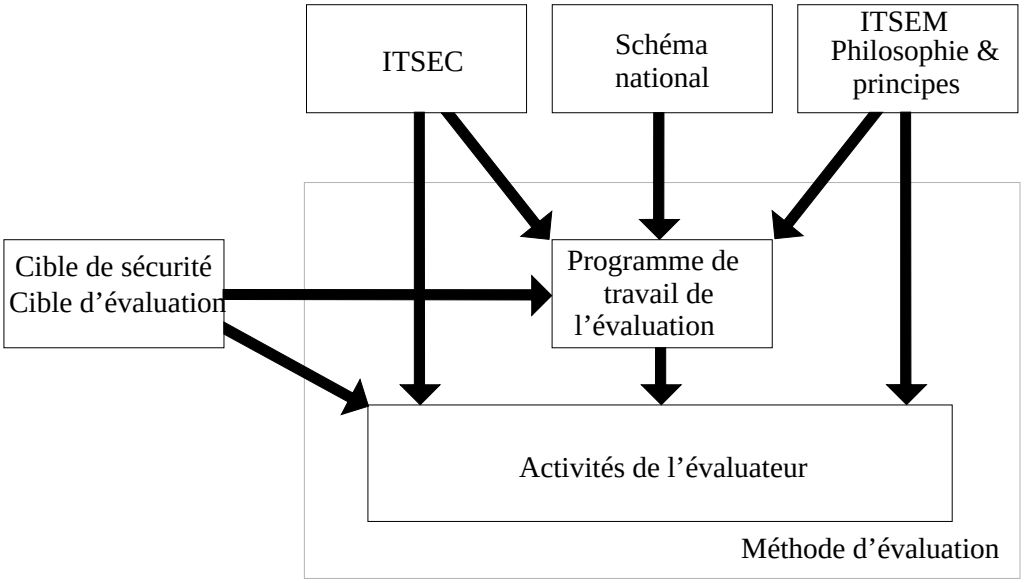


Figure 3.2.1 Élaboration du processus d'évaluation

3.2.16 L'instanciation de la méthode d'évaluation dans un processus d'évaluation particulier est affectée par :

a) les attributs d'évaluation (évaluation simultanée ou consécutive) ;

b) les attributs de la cible d'évaluation (système ou produit).

3.2.17 Ces attributs sont décrits dans la partie 1 de l'ITSEM (1.2.24 - 1.2.28).

Chapitre 3.3 Concepts en sécurité et en évaluation

3.3.1 Dans ce chapitre un certain nombre de concepts et de termes des ITSEC sont explicités en supplément des concepts présentés dans la partie 1 de l'ITSEM, ceci en vue d'une meilleure interprétation de certaines activités de l'évaluateur. Ces concepts et termes sont les suivants :

a) objectifs de sécurité, **biens** et menaces ;

b) conformité et efficacité ;

c) composants, fonctions et mécanismes ;

d) fonctions et composants dédiés, touchant et ne touchant pas à la sécurité ;

e) séparation des fonctionnalités ;

f) raffinement, **erreurs** et correction d'erreur ;

g) **vulnérabilités en exploitation** et de construction ;

h) résistance des mécanismes ;

i) vulnérabilités exploitables ;

j) tests de pénétration.

3.3.2 A noter que les schémas nationaux peuvent fournir une interprétation plus approfondie de ces termes et d'autres encore.

Objectifs de sécurité, biens et menaces

3.3.3 La cible de sécurité spécifie les objectifs de sécurité de la cible d'évaluation en faisant correspondre les menaces et les biens à chaque objectif (il doit exister au moins un objectif de sécurité). Un exemple d'objectif pourrait être :

a) La cible d'évaluation doit empêcher la divulgation des informations sensibles au personnel non suffisament habilité.

b) La cible d'évaluation doit veiller à ce que les responsables chargés de la vérification par recoupement des données du client ne puissent abuser de leur autorité pour, par exemple, commettre des fraudes.

3.3.4 La cible de sécurité énumère les menaces qui pèsent sur la cible d'évaluation et les biens que cette dernière doit protéger. Les ITSEC exigent que les menaces et les biens soient identifiés de sorte que les évaluateurs puissent vérifier que les objectifs de sécurité et les listes de menaces et de biens sont cohérents entre eux.

3.3.5 La cible de sécurité identifie aussi les contre-mesures à réaliser pour protéger les biens contre les menaces de manière à satisfaire aux objectifs de sécurité. Lorsque les contre-mesures doivent être mises en oeuvre à l'aide de moyens techniques, c'est à dire au niveau du système informatique lui-même, elles sont appelées fonctions dédiées à la sécurité. Ces fonctions spécifient la fonctionnalité de sécurité de la cible d'évaluation (plutôt que les mécanismes qui seront utilisés dans la réalisation des fonctions de sécurité). Les ITSEC conseillent de décrire ces fonctions sous les rubriques génériques spécifiées au chapitre 2 des critères ITSEC, ou au moyen d'une classe de fonctionnalité prédéfinie. La cible de sécurité identifie également les objectifs particuliers de chaque contre-mesure (par exemple : la cible d'évaluation utilise une fonction d'identification et d'**authentification** pour établir et vérifier une identité annoncée).

3.3.6 Les menaces spécifiques et les biens sont plus difficiles à spécifier dans la cible de sécurité pour un produit que pour un système. En conséquence, l'argumentaire du produit peut être utilisé par l'acquéreur pour déterminer comment ses biens réels peuvent être protégés de ses menaces réelles par l'utilisation des contre-mesures fournies par le produit. L'argumentaire du produit décrit donc généralement davantage les objectifs de sécurité que les biens et menaces identifiées.

Conformité et efficacité

3.3.7 La notion fondamentale dans les critères ITSEC est la séparation faite entre fonctionnalité et assurance, et pour cette dernière, distinction supplémentaire entre la confiance dans la conformité des fonctions dédiées à la sécurité et la confiance dans l'efficacité de ces fonctions.

3.3.8 Deux questions clefs doivent trouver une réponse pendant une évaluation :

a) Les fournitures démontrent-elles que la cible d'évaluation réalise correctement la cible de sécurité (Conformité) ?

b) Les mesures de sécurité réalisées dans la cible d'évaluation sont-elles efficaces contre les menaces identifiées et sont-elles exemptes de vulnérabilités exploitables (Efficacité) ?

3.3.9 La conformité traite de deux grandes questions :

a) Existe-t-il une description adéquate des fonctions dédiées à la sécurité dans la cible de sécurité, et les fournitures apportent-elles des éléments de preuve que ces fonctions sont correctement réalisées dans la cible d'évaluation ?

b) Une approche disciplinée du développement a-t-elle été suivie, de telle sorte qu'un niveau de confiance adéquat dans le **raffinement correct** des spécifications de besoins puisse être établi ?

3.3.10 L'efficacité doit être considérée comme une liste de contrôle qui comporte divers aspects sur lesquels la cible d'évaluation peut échouer. L'efficacité traite des questions suivantes :

a) Les fonctions dédiées à la sécurité sont-elles capables de protéger les biens spécifiés par rapport aux menaces définies dans la cible de sécurité (Pertinence de la fonctionnalité) ?

b) La conception permet-elle, en supposant la réalisation correcte de chaque fonction dédiée à la sécurité, que la cible d'évaluation dans son ensemble soit sûre comparée à sa cible de sécurité (Cohésion de la fonctionnalité) ?

c) La cible d'évaluation, dans son ensemble et dans son environnement d'exploitation, présente-t-elle des vulnérabilités exploitables (Estimation de la vulnérabilité, résistance des mécanismes et facilité d'emploi) ?

Composants, fonctions et mécanismes

3.3.11 La cible d'évaluation est constituée de composants, lesquels sont eux-mêmes constitués de composants. Les composants identifiés par le développeur au niveau le plus bas de la conception sont appelés des composants élémentaires, comme par exemple les unités de compilation.

3.3.12 Un composant peut réaliser plus d'une fonction. Dans le cas d'un composant élémentaire, les parties qui contiennent la réalisation d'une fonction sont appelées des unités fonctionnelles. Il est important que les fonctions de sécurité identifiées dans la cible de sécurité puissent être mises en correspondance avec des composants à tous les niveaux d'abstraction considérés dans l'évaluation.

3.3.13 La logique ou l'algorithme qui réalise une fonction est appelé(e) un mécanisme. Des considérations sur l'évaluation des mécanismes se trouvent dans l'annexe 6.C de la partie 6.

Fonctions et composants dédiés, touchant et ne touchant pas à la sécurité

3.3.14 Les termes "dédié à la sécurité", "touchant à la sécurité" et "ne touchant pas à la sécurité" s'excluent mutuellement, mais recouvrent le tout, c'est-à-dire que chaque élément de la fonctionnalité d'une cible d'évaluation ne peut être affecté qu'à une et une seule de ces trois catégories. Ces trois attributs s'appliquent aux fonctions comme aux composants.

3.3.15 Des fonctions ne touchent pas à la sécurité si la réalisation des objectifs de sécurité ne dépend pas d'elles. Les fonctions dédiées à la sécurité sont toutes fonctions de la cible d'évaluation qui participent directement aux objectifs de sécurité. Les fonctions touchant à la sécurité contribuent au fonctionnement sûr de la cible d'évaluation et renforcent souvent non seulement les fonctions dédiées à la sécurité, mais également les fonctions qui ne le sont pas. Généralement, les fonctions dédiées à la sécurité reposent sur un fonctionnement correct des fonctions touchant à la sécurité.

3.3.16 Si au moins l'une des fonctions réalisées dans un composant est dédiée à la sécurité, alors ce composant est dédié à la sécurité. Si aucune des fonctions n'est une fonction dédiée à la sécurité ou touchant à la sécurité, alors le composant n'est pas "touchant à la sécurité".

Séparation de la fonctionnalité

3.3.17 La séparation peut être mise en évidence en démontrant (avec la rigueur qui s'impose) que quel que soit le comportement des composants non dédiés à la sécurité, les objectifs de sécurité seront respectés, pourvu que les composants dédiés à la sécurité fonctionnent correctement.

3.3.18 La séparation entre les fonctions dédiées à la sécurité, touchant à la sécurité et ne touchant pas à la sécurité est un élément de la conception générale qui ne dépend pas seulement de la prise en compte de la sécurité. Au moyen du concept de moniteur de référence on sait comment séparer la fonctionnalité répondant à des exigences de confidentialité. Cependant, ce concept ne peut être élargi avec succès aux notions d'intégrité et de disponibilité.

Raffinement, erreurs et correction d'erreur

3.3.19 Les critères ITSEC n'imposent aucune méthode particulière de développement, mais il est supposé que le développement de toute cible d'évaluation comporte plusieurs étapes de raffinement et d'intégration. A la fin du processus de développement, il existe des représentations de la cible d'évaluation à différents niveaux d'abstraction. La cible de sécurité se situe au plus haut niveau d'abstraction. La cible d'évaluation opérationnelle, sous la forme de code exécutable ou de circuit électronique, constitue la représentation la plus concrète et la plus détaillée. Selon les critères de conformité des ITSEC, les termes *cible de sécurité*, *conception générale*, *conception détaillée* et *réalisation* désignent différents niveaux d'abstraction. La conception détaillée, par exemple, est moins abstraite et davantage détaillée que la conception générale. C'est pourquoi on dit que la conception détaillée est un raffinement de la conception générale.

3.3.20 Une fonction décrite dans la cible de sécurité est présente à différents niveaux d'abstraction ou de détail, y compris sa réalisation dans la cible d'évaluation. On dit que la description de cette fonction à un niveau d'abstraction donné de cette hiérarchie est un raffinement correct si la totalité des effets décrits à ce niveau (inférieur) d'abstraction montre les effets décrits au niveau précédent (supérieur) d'abstraction.

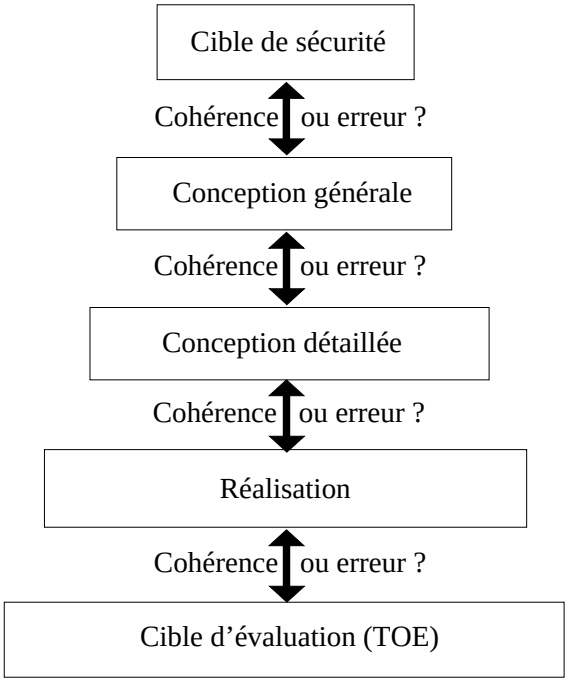


Figure 3.3.1 Représentations de la cible d'évaluation et Conformité

3.3.21 Un échec aux critères de conformité est appelé une erreur. Une incohérence par rapport au raffinement en est une cause caractéristique. Il peut également s'agir d'un problème de traçabilité ou d'incohérence entre deux représentations de la cible d'évaluation (TOE). L'objectif des critères de conformité des ITSEC est d'aider à démontrer que chaque représentation fournie aux évaluateurs constitue un raffinement correct de sa représentation correspondante au niveau supérieur. Les critères de conformité des ITSEC en termes de construction visent à fournir les éléments de preuve que la cible d'évaluation est un raffinement correct de la cible de sécurité. La correspondance entre la cible de sécurité et la cible d'évaluation est fournie par les correspondances qui existent entre les niveaux intermédiaires (comme indiqué dans la figure 3.3.1).

3.3.22 Une erreur est corrigée en modifiant au moins l'une des représentations. Supposons, par exemple, qu'il existe une représentation d'une fonction d'identification et d'authentification à un certain niveau de conception. La conception spécifiera l'action à entreprendre dans le cas d'un débordement des tables contenant les identifiants et les mots de passe des utilisateurs. Si, au niveau inférieur de conception, une action différente est entreprise en cas de débordement des tables, il s'agit d'une erreur dans la mesure où un effet spécifié à un niveau n'existe pas au niveau suivant. Ceci peut avoir deux conséquences.

a) Soit la conception au premier niveau est modifiée de façon à spécifier l'action entreprise au niveau suivant. La conception en amont, telle que la conception générale, voire la cible de sécurité, peut en être affectée.

b) Soit, la conception au niveau suivant est modifiée de façon à spécifier l'action requise au premier niveau. Cette modification affecte généralement la conception et la réalisation en aval.

3.3.23 Une autre cause caractéristique d'erreur est l'insuffisance des éléments de preuve fournis par le commanditaire et le développeur. Les erreurs non décelées peuvent conduire à des vulnérabilités potentielles. Les erreurs typographiques rencontrées dans la documentation du commanditaire et du développeur ne sont généralement pas considérées comme des erreurs au sens des ITSEC.

Vulnérabilités de construction et vulnérabilités en exploitation

3.3.24 Une **vulnérabilité** est une faiblesse de la sécurité d'une cible d'évaluation pouvant être exploitée par un attaquant pour exercer une menace et mettre en danger un bien ou faire échouer une contre-mesure. Il existe des vulnérabilités de construction et des vulnérabilités en exploitation. Les **vulnérabilités de construction** tirent profit de certaines propriétés de la cible d'évaluation qui ont été introduites pendant sa construction, par exemple, l'oubli de l'effacement d'une mémoire tampon. Les **vulnérabilités en exploitation** tirent profit des faiblesses de contre-mesures non techniques pour violer la sécurité d'une cible d'évaluation, par exemple la divulgation du mot de passe d'une personne à une autre.

3.3.25 Le raffinement génère souvent des détails supplémentaires au niveau d'abstraction inférieur. Les effets au niveau inférieur sont un "sur-ensemble" des effets au niveau supérieur. Les détails ajoutés sont une source de vulnérabilités de construction potentielles. Par exemple, l'introduction d'une variable verrou absente au niveau d'abstraction supérieur introduit une vulnérabilité potentielle. Si le contrôle du flux d'information est un objectif de sécurité dans la cible de sécurité et si la variable verrou peut être utilisée pour créer un canal caché, la vulnérabilité peut alors être exploitable.

3.3.26 Les vulnérabilités potentielles issues du raffinement sont identifiées par les évaluateurs au cours de l'examen de la conformité. L'examen des vulnérabilités de construction établit si ces vulnérabilités sont exploitables ou non.

3.3.27 Les vulnérabilités en exploitation concernent la frontière entre les contre-mesures TI et non TI (par exemple : les procédures opérationnelles qui portent sur la sécurité physique, les formes non électronique de la gestion de clefs, la distribution de badges de sécurité). Les évaluateurs seront concernés par les mesures non TI si :

a) celles-ci figurent dans la documentation d'exploitation, ou si

b) la cible de sécurité est formulée sur la base d'une politique de sécurité d'un système (voir les paragraphes 2.8 - 2.15 des ITSEC), ou si elles figurent dans l'argumentaire du produit (voir les paragraphes 2.16 - 2.17 des ITSEC).

3.3.28 Les contre-mesures non TI sur lesquelles repose la sécurité de la cible d'évaluation sont identifiées sous la forme d'affirmations sur l'environnement de la cible d'évaluation. Il peut être affirmé, par exemple, que seuls les employés d'une société sont autorisés à avoir accés au système et qu'il est de la responsabilité des contre-mesures non TI d'assurer que cette assertion soit satisfaite. Les évaluateurs supposent que cette affirmation est vraie. Si la combinaison de contre-mesures TI et non TI est dans le champ d'application de l'évaluation, les évaluateurs devraient déterminer si la combinaison comporte des vulnérabilités potentielles.

Résistance des mécanismes

3.3.29 Les définitions des ITSEC qui concernent les trois cotations de la résistance des mécanismes *élémentaire*, *moyenne* et *élevée* constituent une échelle grossière qui permet d'exprimer les besoins des utilisateurs. Les définitions ne fournissent pas un moyen détaillé pour effectuer une estimation au cours de l'évaluation. Il convient d'établir une distinction entre le volume des efforts à fournir pour découvrir une vulnérabilité, celui pour trouver une description de la vulnérabilité (par exemple : dans un article de magazine), et enfin celui pour exploiter une vulnérabilité fondée sur cette description. La cotation met l'accent sur l'effort à fournir pour exploiter une vulnérabilité.

3.3.30 La cotation de la résistance des mécanismes que l'évaluateur établit, s'estime en termes de compétence, d'opportunité et de ressources. De manière plus pratique, les quatre paramètres compétence, collusion, temps et équipement peuvent être utilisés.

3.3.31 La cotation doit être calculée pour toutes les combinaisons possibles et bien fondées des valeurs de ces paramètres. Pour ce faire, on pourra recourir à l'utilisation de tableaux ou d'un ensemble de règles. Des précisions sur l'estimation de la résistance des mécanismes, sont présentées à l'annexe 6.C de la partie 6.

3.3.32 Les mécanismes cryptographiques ne sont pas cotés par les CESTI (voir le paragraphe 3.23 des ITSEC).

Vulnérabilités exploitables

3.3.33 Il peut exister plusieurs façons de faire échouer une contre-mesure donnée, certaines sont plus faciles que d'autres. Généralement, un attaquant doit mettre en échec plus d'une contre-mesure pour réussir l'attaque de la cible d'évaluation. Le développeur anticipe les chemins par lesquels la cible d'évaluation peut être attaquée et choisit les contre-mesures en conséquence. En fonction de l'analyse du développeur, les évaluateurs mènent indépendamment une étude de la cible d'évaluation, du point de vue d'un attaquant, pour déterminer toutes les possibilités qui peuvent compromettre un objectif de sécurité.

3.3.34 Une pénétration réussie révèle une vulnérabilité exploitable ou une défaillance de la résistance des mécanismes exigée. S'il existe une attaque réussie, la vulnérabilité est exploitable. Dans l'intérêt d'un bilan économique correct pour l'évaluation, il n'est pas besoin de faire la preuve du caractère exploitable d'une vulnérabilité au moyen de tests si les arguments théoriques sont suffisants. Des scénarios d'attaque sont élaborés et des tests de pénétration sont effectués dans le cadre de l'estimation de la vulnérabilité au cours de l'évaluation.

Tests de pénétration

3.3.35 Quand les évaluateurs ont établi la liste des vulnérabilités potentielles et l'ont comparée avec la liste fournie par le développeur (voir paragraphe 3.12 des ITSEC), les évaluateurs achèvent leur analyse indépendante par des tests de pénétration pour vérifier si les vulnérabilités potentielles sont exploitables.

3.3.36 Les tests de pénétration diffèrent des tests fonctionnels, lesquels visent à démontrer que la cible d'évaluation est conforme à sa spécification.

Chapitre 3.4 Principes de la conduite des évaluations

Théorie et expérience

3.4.1 Les théories à propos de la cible d'évaluation et de son comportement pourraient aider les évaluateurs à comprendre comment la cible d'évaluation satisfait à sa cible de sécurité. Les évaluateurs devraient élaborer et consigner leurs théories concernant la cible d'évaluation au cours de l'analyse des fournitures. Ces théories devraient être adoptées et confirmées, ou rejetées au vu d'autres informations sur la cible d'évaluation, ou de manière expérimentale au moyen des tests de pénétration et d'autres tests.

3.4.2 Dans le domaine de la science, l'expérience est guidée par une hypothèse que l'on cherche alors à vérifier. De telles expériences peuvent s'inscrire dans l'une des catégories suivantes :

a) des essais pour montrer que le système considéré présente ou non certaines propriétés ;

b) des tentatives pour distinguer des théories concurrentes sur le comportement d'un système au moyen de la conception et de la réalisation d'expériences pour vérifier ou réfuter ces différentes théories.

3.4.3 Ce principe à propos des expériences et des théories peut s'appliquer à la pratique de l'évaluation. Les tests d'une cible d'évaluation ne doivent pas être effectués au hasard, mais doivent être régis par une théorie à vérifier ou un doute à dissiper. Il existe plusieurs manières de procéder pour les évaluateurs. À partir de l'analyse de la cible de sécurité, les évaluateurs devraient parvenir à une compréhension des propriétés de sécurité exigées de la cible d'évaluation et exploiter ces informations pour développer les tests. À partir de l'analyse des autres fournitures de l'évaluation, les développeurs devraient parvenir à une compréhension du comportement de la cible d'évaluation et exploiter ces informations pour développer les tests qui confirment ou infirment le caractère exploitable des vulnérabilités potentielles. La connaissance du comportement de produits et de systèmes similaires est un autre moyen important pour développer des tests.

Décomposition systématique

3.4.4 La complexité d'une cible d'évaluation est pratiquement illimitée. La décomposition systématique constitue une approche reconnue pour faire face à ce problème au cours de l'évaluation. Cette approche se manifeste dans diverses exigences des ITSEC pour le développeur qui concernent les fournitures d'évaluation et le processus de développement. A titre d'exemple :

a) le découpage de la définition de la fonctionnalité de sécurité exigée, en fonctions dédiées à la sécurité dans la cible de sécurité ;

b) la séparation au niveau de la conception générale entre la fonctionnalité de sécurité et les autres fonctionnalités ;

c) l'utilisation d'un processus de construction par phases ;

d) l'utilisation d'approches de développement structuré ;

e) l'utilisation de langages de programmation qui encouragent la décomposition modulaire.

3.4.5 Les ITSEC respectent également le principe de décomposition systématique au cours de l'évaluation en séparant les aspects de conformité et d'efficacité et en distinguant différents aspects de l'efficacité tels que la pertinence, la cohésion, etc.

Modélisation

3.4.6 La modélisation est utilisée comme une technique d'évaluation qui étaye une théorie et prouve la compréhension. Elle est particulièrement adaptée aux niveaux d'évaluation les plus élevés. Le développement de modèles est souvent fondé sur l'expérience et l'intuition. Ces modèles sont décrits à l'aide de spécifications dont le style est soit informel, soit semi-formel ou soit formel. Les modèles fournis par le commanditaire/développeur devraient être utilisés par les évaluateurs comme base de leur propre compréhension et de leur propre modélisation.

Traçabilité

3.4.7 Pour les niveaux d'évaluation les plus élevés, la réalisation des objectifs de sécurité devrait être complètement traçable par les évaluateurs en descendant jusqu'à la cible d'évaluation opérationnelle. Cette traçabilité ne peut être complète que si elle couvre toutes les phases de développement, à savoir les phases de spécification de besoins, de conception générale, de conception détaillée et de réalisation. La traçabilité doit être fournie par la cible de sécurité et les autres fournitures qui fournissent différentes représentations de la cible d'évaluation. Ceci couvre également le code source et le code exécutable le cas échéant, en fonction du niveau d'évaluation et de la cible d'évaluation.

Verdicts

3.4.8 Au vu des critères ITSEC, une cible d'évaluation ne réussit l'évaluation que si elle obtient des verdicts de réussite pour tous les critères de conformité et d'efficacité qui correspondent au niveau d'évaluation visé. Ceci implique qu'il ne subsiste dans la phase de conclusion de l'évaluation aucune vulnérabilité exploitable dans la cible d'évaluation opérationnelle, et que la résistance minimum des mécanismes annoncée soit atteinte. L'évaluation échoue si, à la fin du processus, l'un des critères de conformité n'est pas satisfait ou s'il subsiste une vulnérabilité exploitable dans la cible d'évaluation.

3.4.9 Pour prononcer un verdict par rapport à un critère des ITSEC, les évaluateurs ont pour point de départ les éléments de preuve apportés par le commanditaire dans les fournitures. Ce point de départ est complété par des tâches de l'évaluateur additionnelles conformément aux critères ITSEC, généralement au moyen d'une vérification par recoupement ou au moyen des tests de pénétration, de façon à apporter des éléments indépendants de preuve du respect du critère et de façon à contrôler ainsi la validité des éléments de preuve du commanditaire/développeur. Ce principe d'indépendance s'applique à l'ensemble des résultats d'analyse et de test du commanditaire/développeur, par exemple en confirmant les résultats de tests, par le rejeu de certains d'entre eux. Un verdict d'échec est délivré lorsque le commanditaire/développeur ne fournit pas d'élément de preuve, ou fournit des éléments de preuve incomplets (principe de complétude) ou incorrects pour un critère pertinent.

Correction des erreurs

3.4.10 Si une erreur est détectée au cours de l'évaluation, il est nécessaire de la corriger ; à défaut de quoi l'évaluation rendra le verdict d'échec pour l'un des critères de conformité. Ceci vaut aussi pour les vulnérabilités exploitables.

3.4.11 Les corrections apportées aux fournitures déjà évaluées invalideront certains des travaux d'évaluation précédents en entraînant la répétition des travaux d'évaluation.

Tests de pénétration

3.4.12 Les tests de pénétration offrent une assurance indépendante qu'une cible d'évaluation spécifique ne comporte ni vulnérabilités exploitables ni mécanismes critiques ayant une résistance des mécanismes inférieure à celle qui est annoncée.

3.4.13 Les tests de pénétration constituent le point culminant du processus suivant :

a) obtenir progressivement une compréhension de la cible d'évaluation et de la cible de sécurité en exécutant les tâches de l'évaluateur qui concernent la conformité ;

b) rechercher des vulnérabilités et émettre des hypothèses qui concernent leur exploitation en exécutant les tâches de l'évaluateur concernant l'efficacité.

3.4.14 Les tests de pénétration sont effectués pour toutes les évaluations et constituent généralement la tâche finale de l'évaluateur. Les évaluateurs identifient, spécifient, exécutent et enregistrent les tests de pénétration.

Listes de contrôle

3.4.15 Les listes de contrôle qui sont utilisées dans les évaluations peuvent assurer qu'aucune question classique à prendre en compte (par exemple : des vulnérabilités bien connues dans un certain type de produit ou système) n'a été oubliée avant que le verdict ne soit prononcé.

Revue

3.4.16 Les évaluations exigent réflexion et jugement. Afin de limiter les biais et les conséquences d'erreurs et pour assurer une qualité d'ensemble, les résultats des activités d'évaluation doivent faire l'objet d'un processus de revue au sein du CESTI. Les exigences qui concernent le processus de revue et l'implication de l'**organisme de certification** pourraient être détaillées dans le schéma national. La revue doit impliquer au moins une personne qui n'a pas participé à la production de ces résultats.

3.4.17 L'objet du processus de revue de l'évaluation est d'assurer que les résultats de l'évaluation sont en accord avec les critères considérés, les exigences de l'ITSEM et le schéma national.

Enregistrements

3.4.18 Des enregistrements complets sont exigés pour fournir des éléments de preuve du travail d'évaluation et des résultats. Les décisions importantes, les arguments, les tests et leurs résultats doivent être décrits par exemple dans des rapports ou des journaux de consignation. La documentation des problèmes temporaires et de leur résolution ou des tâches effectuées indépendamment par les évaluateurs peut être considérée comme utile et comme une source de confirmation. Les règles du schéma national d'évaluation et de certification peuvent s'appliquer à ces aspects.

Ressources

3.4.19 Les ressources qui sont nécessaires pour une évaluation, dépendent principalement de la complexité de la cible d'évaluation, de sa cible de sécurité et du niveau d'évaluation. D'autres facteurs qui déterminent la quantité de ressources nécessaire sont la compétence et l'expérience des évaluateurs et l'utilisation d'outils en appui. Les tâches de l'évaluateur nécessaires découlent de l'ensemble des critères à considérer, de la structure de la cible d'évaluation et des fournitures d'évaluation. L'efficacité économique est une préoccupation du CESTI. Les exigences minimales pour les ressources sont de la compétence du schéma national et devraient reposer sur une expérience pratique.

Ressources pour les tests de pénétration

3.4.20 La recherche de vulnérabilités exploitables est limitée par la quantité d'informations fournie en fonction du niveau d'évaluation et par le niveau de compétence, l'opportunité et les ressources qui correspondent à la résistance minimum des mécanismes annoncée.

Programme de travail pour l'évaluation

3.4.21 Un programme de travail pour l'évaluation détaille les activités de l'évaluateur, estime les ressources nécessaires et établit une planification. Des conseils pour rédiger un programme de travail de l'évaluation sont données dans la partie 4 de l'ITSEM.

Répétabilité, reproductibilité, impartialité, et objectivité

3.4.22 La répétabilité, la reproductibilité, l'impartialité et l'objectivité sont des principes qui méritent un effort particulier dans la conduite des évaluations. Ils sont fortement liés les uns aux autres, notamment l'impartialité et l'objectivité d'une part, et la reproductibilité et la répétabilité d'autre part. L'impartialité et l'objectivité sont des conditions préalables à la reproductibilité et la répétabilité. La figure 3.4.1 illustre cet aspect.

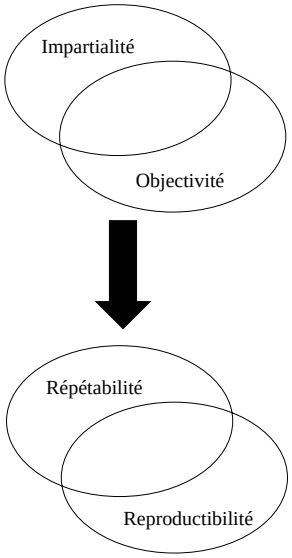


Figure 3.4.1 Quatre principes élémentaires en évaluation

3.4.23 L'utilisation de procédures, de techniques et d'outils d'évaluation normalisés et documentés permet d'appliquer les quatre principes élémentaires (voir la partie 4 de l'ITSEM). Les aspects de l'efficacité tels que l'identification des vulnérabilités, la résistance des mécanismes et le caractère exploitable des vulnérabilités nécessitent une attention particulière, car ils introduisent des facteurs subjectifs comme l'expérience et l'intuition. La subjectivité ne peut être totalement éliminée du processus d'évaluation. Elle nécessite l'implication d'une partie qui a un regard indépendant sur les évaluations, tel qu'un organisme de certification qui assurera la cohérence des résultats de différents CESTI ainsi que la possibilité de les comparer (voir la partie 2 de l'ITSEM).

Partie 4 Processus d’évaluation

Table des matières

Figures

Chapitre 4.1 Introduction

Méthodes d'évaluation

4.1.1 Cette partie de l'ITSEM s'adresse plus particulièrement aux évaluateurs. Elle décrit les méthodes utilisées dans les évaluations en s'attachant à la fois au cadre organisationnel et aux techniques utilisées pour évaluer les cibles d'évaluation selon les critères ITSEC. Elle décrit également les données, le processus et les résultats de l'évaluation. Elle ne donne pas une description exhaustive de la façon dont chaque tâche de l'évaluateur est effectuée.

4.1.2 Certains passages de cette partie de l'ITSEM définissent les aspects imposés des méthodes d'évaluation (ces aspects sont clairement identifiés dans le texte par ***les passages grisés écrits en caractères gras***[1]). L'objectif de ces règles obligatoires est d'assurer que les évaluations menées selon les critères ITSEC et l'ITSEM disposent d'une base technique commune.

Organisation

4.1.3 Cette partie comporte plusieurs chapitres, ces remarques préliminaires constituent le chapitre 4.1.

4.1.4 Le chapitre 4.2 fournit une vue d'ensemble du processus d'évaluation qui identifie les rôles joués par les parties impliquées dans l'évaluation et décrit le processus dans ses phases successives.

4.1.5 Le chapitre 4.3 décrit les dispositions qui concernent le lancement de l'évaluation et l'obtention des **fournitures**.

4.1.6 Le chapitre 4.4 contient une description détaillée du processus d'évaluation du point de vue des évaluateurs. Le niveau de détail donné est celui qui est nécessaire pour permettre l'équivalence technique des évaluations.

4.1.7 Le chapitre 4.5 traite des techniques et des outils qui peuvent être utiles aux évaluateurs.

4.1.8 Le chapitre 4.6 donne des avis aux évaluateurs sur la réutilisation des résultats d'évaluation.

4.1.9 Le chapitre 4.7 spécifie les résultats qu'une évaluation devrait produire, à savoir les **Rapports Techniques d'Évaluation** (RTEs).

1. NdT : ces passages sont écrits dans une police de caractères différente et en italique gras.

Chapitre 4.2 Le processus d'évaluation

Introduction

4.2.1 Le présent chapitre fournit une vue d'ensemble du processus d'évaluation en définissant les rôles des parties impliquées dans le processus, ainsi que les phases et les étapes que parcourt le processus.

4.2.2 Le processus d'évaluation décrit dans ce chapitre doit être considéré comme un cadre qui décrit les aspects d'organisation et de procédures à suivre lors de la conduite d'une évaluation.

Rôles

Généralités

4.2.3 Le processus d'évaluation décrit dans ce chapitre nécessite l'existence des entités suivantes :

a) centre d'évaluation de la sécurité des technologies de l'information (CESTI) ;

b) commanditaire ;

c) développeur ;

d) **organisme de certification**.

4.2.4 Le rôle de chacune de ces entités dans le processus d'évaluation est décrit dans les sous-sections suivantes. La figure 4.2.1 représente ces entités et les informations qui peuvent circuler entre elles au cours du processus d'évaluation.

CESTI

4.2.5 Le rôle du CESTI est d'agir comme un organisme indépendant au sein duquel les évaluations par des tiers peuvent être réalisées dans le cadre du **schéma national**. Le CESTI traite les aspects organisationnels, administratifs et contractuels des évaluations.

4.2.6 Le rôle des évaluateurs au sein du CESTI est d'effectuer une inspection impartiale et détaillée d'une cible d'évaluation à la recherche de **vulnérabilités** et de déterminer dans quelle mesure sa réalisation satisfait sa cible de sécurité, conformément aux ITSEC. Les résultats de l'évaluation sont communiqués à l'organisme de certification et au commanditaire.

4.2.7 ***Les évaluateurs réalisent les travaux d'évaluation conformément aux exigences des ITSEC et de l'ITSEM et aux pratiques et procédures établies par le schéma national. Au cours de ces travaux, les évaluateurs sont tenus responsables de :***

a) ***conserver un enregistrement de tous les travaux effectués au cours de l'évaluation ;***

b) ***produire les rapports d'évaluation ;***

c) ***maintenir la confidentialité nécessaire à tous les aspects des travaux d'évaluation.***

4.2.8 Les évaluateurs fournissent une assistance à l'organisme de certification lors du processus de certification (voir la sous-section *Phase III Conclusion* du présent chapitre).

4.2.9 Les évaluateurs assurent la liaison avec les autres parties impliquées dans l'évaluation, qui comprennent le commanditaire de l'évaluation, le développeur de la cible d'évaluation et l'organisme de certification.

4.2.10 Les évaluateurs devraient assurer que le commanditaire et le(s) développeur(s) sont informés des obligations qui leur ont été imposées par le schéma national et qu'ils les ont parfaitement comprises. Les évaluateurs devraient assurer, en particulier, que le commanditaire est capable de fournir toutes les données nécessaires au processus d'évaluation (fournitures). Par conséquent, au début d'une évaluation, les évaluateurs devraient clairement identifier ce que le commanditaire doit fournir.

Commanditaire

4.2.11 Le commanditaire d'une évaluation est généralement le fournisseur d'un produit, ou l'utilisateur ou le fournisseur d'un système, désireux de démontrer que la cible d'évaluation satisfait la cible de sécurité spécifiée.

4.2.12 Le commanditaire est à l'origine de l'évaluation d'une cible d'évaluation par un CESTI. Il définit la cible de sécurité, commande l'évaluation, reçoit le RTE et si à l'issue de l'évaluation un verdict de réussite est rendu, le **certificat/rapport de certification**.

4.2.13 Le rôle du commanditaire est détaillé dans la partie 6 de l'ITSEM.

Développeur

4.2.14 Le terme développeur fait référence à l'organisation (ou aux organisations) qui produit la cible d'évaluation (ou des composants de la cible d'évaluation). Le développeur (s'il ne commandite pas aussi l'évaluation) devrait être prêt à coopérer avec le commanditaire et accepter d'apporter son aide lors de l'évaluation en fournissant, par exemple, une assistance technique au CESTI.

4.2.15 Le rôle du développeur est décrit plus en détail dans la partie 6 de l'ITSEM.

Organisme de certification

4.2.16 Les principaux objectifs d'un organisme de certification sont de :

a) créer les conditions qui permettent que, dans le cadre d'un schéma, les travaux de tous les CESTI soient exacts et cohérents et que leurs conclusions satisfassent aux exigences de validité, de répétabilité et de reproductibilité ;

b) fournir une confirmation indépendante qui atteste que les évaluations ont été menées conformément aux procédures, méthodes et critères approuvés.

4.2.17 Le rôle de l'organisme de certification est décrit plus en détail dans la partie 2 de l'ITSEM.

Les phases du processus d'évaluation

Généralités

4.2.18 Le processus d'évaluation peut être divisé en trois phases : préparation, conduite et conclusion. Ces trois phases sont décrites en détail dans les sous-sections suivantes.

Phase I - Préparation

4.2.19 Le commanditaire entre en relation avec l'organisme approprié dans le cadre du schéma national (organisme de certification ou CESTI) et lance l'évaluation d'une cible d'évaluation. Un CESTI est choisi pour effectuer la phase I sous contrat avec le commanditaire. Le commanditaire fournit au CESTI sa cible de sécurité pour la cible d'évaluation (éventuellement sous une forme provisoire) et définit le champ de l'évaluation.

4.2.20 Le CESTI estime la probabilité de réussite d'une évaluation, en demandant des informations appropriées au commanditaire. Si le résultat est satisfaisant, le CESTI passera un contrat avec le commanditaire pour réaliser l'évaluation. Le CESTI peut éventuellement passer en revue la cible de sécurité et aviser le commanditaire à propos des changements nécessaires à l'établissement d'une base solide pour l'évaluation.

4.2.21 Les schémas nationaux peuvent exiger des CESTI qu'ils préparent un **programme de travail pour l'évaluation** (PTE) ou une liste des fournitures avant de commencer l'évaluation. Un PTE décrit les travaux que le CESTI effectuera lors de l'évaluation. Une liste des fournitures comprend une description des fournitures que le commanditaire est tenu de délivrer au CESTI au cours de l'évaluation, ainsi que les dates auxquelles elles seront exigées. L'organisme de certification passera en revue le PTE afin de vérifier que les travaux proposés sont appropriés. L'avantage des PTE et des listes des fournitures est que le commanditaire et le CESTI peuvent être clairs, dès le début, sur le travail à réaliser.

4.2.22 Au début d'une évaluation, un PTE ne peut être établi qu'à partir des informations mises à la disposition du CESTI à ce moment-là. Au fur et à mesure que l'évaluation progresse, on peut s'attendre à une augmentation de la quantité d'informations mises à la disposition des évaluateurs, et donc à l'évolution du PTE. L'organisme de certification passera en revue les modifications apportées au PTE pour veiller à ce que les travaux proposés restent appropriés.

4.2.23 Les CESTI peuvent donner un avis aux commanditaires et aux développeurs sur la manière de produire les fournitures nécessaires à l'évaluation. Les avis peuvent provenir d'un CESTI différent de celui qui réalise l'évaluation. ***Si un CESTI donne des avis, ces derniers ne doivent en aucun cas affecter l'indépendance du CESTI dans une quelconque évaluation.*** Les détails à ce sujet seront donnés par les schémas nationaux.

4.2.24 Lors de la phase de préparation, le commanditaire et le CESTI devraient se mettre d'accord sur le besoin, dans le RTE, d'informations en vue d'une réévaluation.

Phase II - Conduite

4.2.25 Avant de commencer la phase de conduite, un contrat devrait avoir été signé entre le commanditaire et le CESTI, les travaux exigés devraient avoir été compris et la cible de sécurité devrait être stabilisée.

4.2.26 Pour chaque phase ou chaque aspect approprié des ITSEC, les évaluateurs exécutent les tâches d'évaluation éxigées. Les fournitures sont vérifiées afin de voir si chaque critère est traité. De plus, les évaluateurs établissent une liste de **vulnérabilités potentielles**. Tous les problèmes identifiés seront discutés entre les parties concernées.

4.2.27 Les problèmes identifiés au cours de la phase de conduite se répartissent en deux groupes distincts. Le premier groupe présente les problèmes auxquels le commanditaire est capable d'apporter une solution acceptable par le CESTI et l'organisme de certification. Le CESTI et le commanditaire se mettent d'accord sur le délai nécessaire à la résolution du problème conformément à la solution proposée. Le deuxième groupe représente les problèmes que le commanditaire ne peut ou ne veut pas résoudre. Le CESTI et l'organisme de certification informent le commanditaire des conséquences éventuelles en cas d'absence de solutions. Le commanditaire peut alors soit renoncer à l'évaluation, soit accepter les conséquences pour la certification.

4.2.28 ***Au cours d'une évaluation, le CESTI doit produire son RTE.*** Le RTE est le produit final de l'évaluation, mais ne représente pas le produit final du processus d'évaluation et de certification. La version finale du RTE est remise au commanditaire et à l'organisme de certification pour approbation.

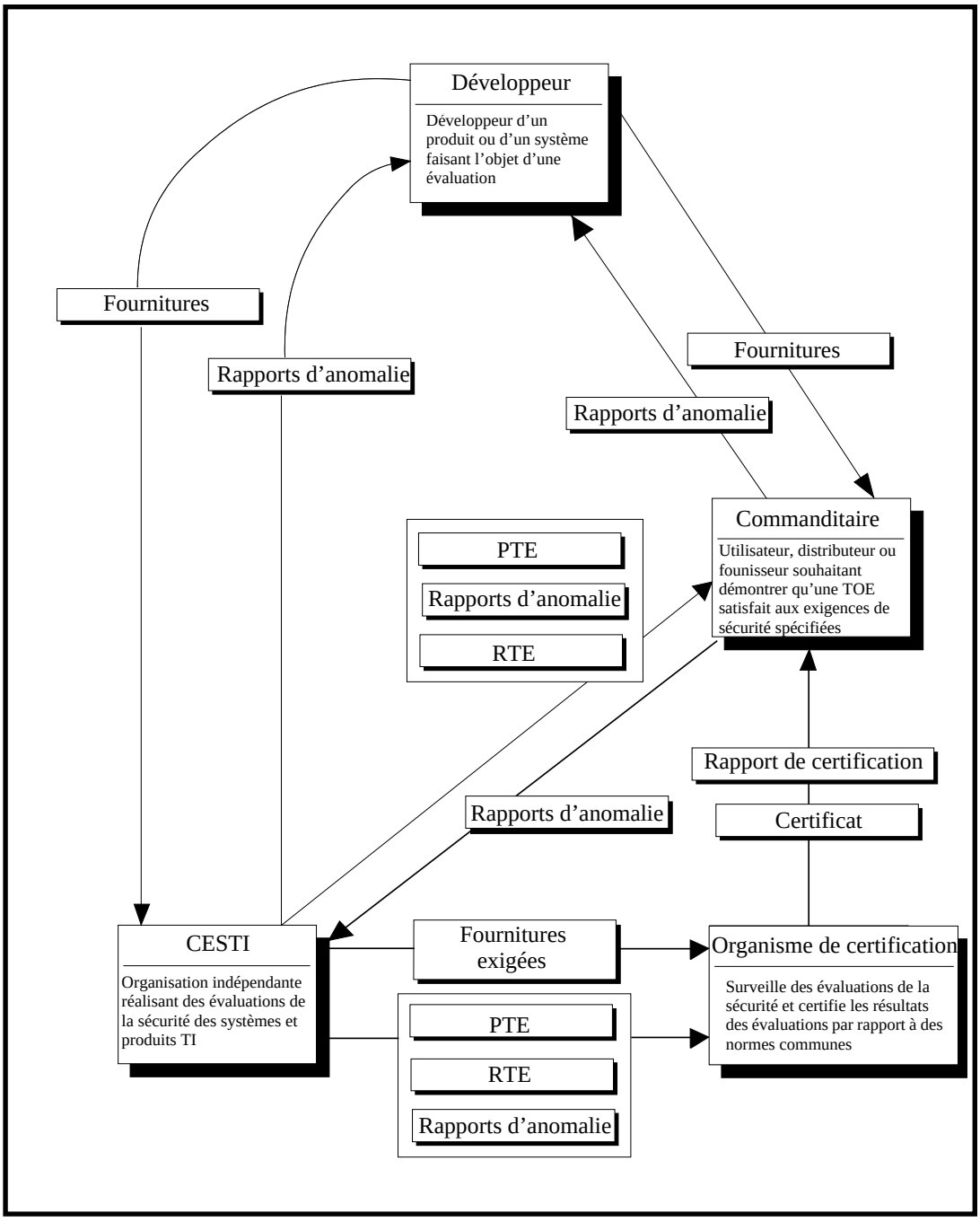
Phase III - Conclusion

4.2.29 Dans la phase de conclusion, le CESTI fournit la version approuvée du RTE à l'organisme de certification et au commanditaire pour valoir comme un enregistrement des résultats de l'évaluation. Le RTE peut également servir à de futurs évaluateurs, si la cible d'évaluation est réévaluée. Le RTE, ou toute partie de celui-ci, sous sa forme provisoire ou finale, devrait être traitée de manière confidentielle.

4.2.30 L'organisme de certification peut demander au CESTI qu'il fournisse une assistance technique, et peut demander, dans les limites du raisonnable, à avoir accès à des résultats et éléments de preuve techniques spécifiques pour soutenir les conclusions présentées dans le RTE. Normalement cela n'entrainera pas le CESTI dans des travaux d'évaluation supplémentaires.

4.2.31 Pendant le processus de certification, l'organisme de certification examine le RTE afin de déterminer si la cible d'évaluation satisfait sa cible de sécurité, en tenant compte de tous les facteurs extérieurs au champ d'application de l'évaluation. Participant au processus, il est capable d'attribuer un niveau d'évaluation. Ses conclusions sont enregistrées dans le certificat/rapport de certification.

4.2.32 ***L'enlèvement des fournitures doit être fait dans cette phase.***



Note : un commanditaire peut également être développeur

Figure 4.2.1 Exemple de flux d'informations au cours du processus d'évaluation

Chapitre 4.3 Données de l'évaluation

Introduction

4.3.1 Le présent chapitre décrit les éléments que les évaluateurs devraient prendre en considération avant et pendant le lancement d'une évaluation. Il s'intéresse à comment les évaluateurs apportent leur concours au commanditaire dans la fourniture des données pour l'évaluation et ce que les évaluateurs font des fournitures, en termes de traitement, une fois qu'elles ont été reçues.

4.3.2 L'objectif de ce chapitre n'est pas d'imposer une organisation pour les schémas nationaux, mais plutôt de fournir aux évaluateurs des informations, sur la manière caractéristique de lancer une évaluation et d'en traiter ses fournitures.

4.3.3 Il devrait être noté que, s'il n'est pas obligatoire de lancer une évaluation sous les auspices de l'organisme de certification, il est recommandé de l'impliquer dans l'évaluation aussitôt qu'il est raisonnable de le faire afin de minimiser les risques techniques et commerciaux de l'évaluation.

4.3.4 Le terme *de fourniture* est employé pour désigner tout élément (y compris la cible d'évaluation elle-même) qu'il est demandé de mettre à la disposition des évaluateurs dans le cadre de l'évaluation. Cela comprend les éléments intangibles, tels que l'aide fournie aux évaluateurs et l'accès aux systèmes informatiques. L'annexe 6.A de la partie 6 devrait être consultée pour plus de détails sur les exigences de l'ITSEM et des ITSEC qui traitent des fournitures.

4.3.5 L'objectif des fournitures est de permettre aux évaluateurs d'évaluer la cible d'évaluation. Différents types de fournitures contribuent à atteindre cet objectif de diverses manières, par exemple :

a) les fournitures peuvent apporter des éléments de preuve d'efficacité ou de conformité, par exemple, une description informelle de la correspondance entre la conception détaillée et le code source ;

b) les fournitures peuvent permettre aux évaluateurs d'établir des éléments complémentaires de preuve de conformité ou d'efficacité, par exemple, l'accès à la cible d'évaluation développée ;

c) les fournitures peuvent améliorer le rendement global du travail des évaluateurs, par exemple, l'assistance technique du développeur.

Responsabilités pour les fournitures

4.3.6 La responsabilité de fournir toutes les fournitures requises pour une évaluation incombe au commanditaire. Cependant, les fournitures seront, pour la plupart d'entre elles, produites et fournies par le développeur (lorsque le commanditaire n'est pas le développeur). Les évaluateurs ne sont pas concernés par les relations contractuelles entre le commanditaire et le(s) développeur(s). Le commanditaire est le client des évaluateurs.

4.3.7 Les coûts et les risques d'exploitation (par exemple, les pertes ou les dommages causés par le feu, l'eau, le vol, etc.) de toutes les fournitures devraient relever de la responsabilité du commanditaire, sauf accord contraire établi avec les évaluateurs. A noter que certaines fournitures, telles que des types nouveaux ou particuliers de matériels, peuvent avoir un coût de remplacement difficile à déterminer et peuvent présenter des risques à assurer qui ne peuvent être transférés aux évaluateurs.

4.3.8 Il est recommandé que les évaluateurs produisent une liste des fournitures. Il s'agit d'une liste définitive des fournitures de l'évaluation prévues (par exemple, un ensemble de références à la documentation du commanditaire) qui mentionnent les dates auxquelles les fournitures sont censées être mises à la disposition des évaluateurs. La liste des fournitures peut être mise en référence dans le RTE.

4.3.9 Il est recommandé que les objectifs pour le lancement de l'évaluation soient clairement compris par les évaluateurs et communiqués aux autres parties. Par conséquent, il est recommandé que les évaluateurs s'assurent que, toutes les parties impliquées dans l'évaluation ont une compréhension commune de l'objectif et de la portée de l'évaluation et qu'elles sont conscientes de leurs responsabilités.

4.3.10 Des exemples de points à traiter éventuellement avec un commanditaire comprennent le niveau de sensibilité des informations sur le plan national ainsi que leur confidentialité commerciale, l'accès aux outils spécialisés et les exigences les concernant, toutes les limitations imposées quant à l'accès des évaluateurs aux fournitures de l'évaluation, tous les résultats d'évaluation précédents et la fréquence désirée des réunions d'avancement.

4.3.11 Pour établir un arrangement particulier entre un CESTI et un commanditaire, les points suivants devront probablement être précisés :

a) le support et le format des fournitures informatiques ;

b) le programme pour la production des fournitures ;

c) le nombre d'exemplairesde fournitures à livrer ;

d) la position à adopter quant aux fournitures provisoires ;

e) la position à adopter quant aux produits à utiliser conjointement avec la cible d'évaluation ;

f) les accords qui concernent les discussions sur l'environnement de développement avec le développeur ;

g) l'accès aux sites de développement et au site d'exploitation ;

h) le type et la durée de l'assistance du développeur, y compris l'accès aux systèmes informatiques et les besoins en locaux pour les évaluateurs.

4.3.12 Dans de nombreux cas, les évaluateurs devront pouvoir accéder aux informations fournies par des sous-traitants ou des tiers. Le commanditaire devrait prendre en compte ces cas de figure.

4.3.13 Le type d'évaluation, simultanée ou consécutive, influera sur la disponibilité des fournitures et devra être pris en compte lors de la production d'un PTE spécifique (voir chapitre 4.4).

4.3.14 Le type de cible d'évaluation, système ou produit, influera également sur la livraison des fournitures et donc sur la production d'un PTE spécifique. Par exemple, un produit peut être disponible pour être installé et testé au CESTI, tandis qu'un système a très peu de chances d'être mis à la disposition du CESTI de la même manière.

Gestion des fournitures

Confidentialité

4.3.15 Lors de leurs travaux, les CESTI auront accès à des informations sensibles sur le plan commercial pour leurs clients et pourront obtenir l'accès à des informations sensibles sur le plan national. Les partenaires de l'évaluation doivent avoir l'assurance que les informations délivrées aux CESTI ne seront pas détounées.

4.3.16 Les exigences générales de confidentialité concernent les schémas nationaux. Les commanditaires et les CESTI peuvent se mettre d'accord sur des exigences supplémentaires pour autant qu'elles soient cohérentes avec le schéma national.

4.3.17 Les exigences de confidentialité affecteront de nombreux aspects des travaux d'évaluation, y compris la réception, la gestion, le stockage et la restitution des fournitures.

Fournitures provisoires

4.3.18 Les évaluateurs exigent des versions stables et définitives des fournitures. Cependant, dans certains cas, l'accès à des versions provisoires de fournitures particulières peut être utile aux évaluateurs, par exemple :

a) la documentation des tests afin de permettre aux évaluateurs d'établir une première estimation des tests et des procédures de test ;

b) le code source ou les schémas de matériel afin de permettre aux évaluateurs d'estimer l'application des normes du développeur.

4.3.19 Le recours aux fournitures provisoires est plus fréquent quand l'évaluation d'une cible d'évaluation est effectuée en parallèle à son développement. Cependant, on peut également y avoir recours pour l'évaluation consécutive d'un produit ou d'un système pendant laquelle le développeur a dû effectuer des travaux supplémentaires pour résoudre un problème identifié par les évaluateurs (par exemple, corriger une **erreur** dans la construction) ou pour fournir des éléments de preuve de sécurité qui n'apparaissent pas dans la documentation existante (par exemple, les fournitures liées à l'efficacité dans le cas d'un produit ou d'un système qui n'a pas été développé à l'origine pour satisfaire aux exigences des ITSEC).

Gestion de configuration

4.3.20 ***Les évaluateurs doivent exercer un contrôle sur les fournitures de l'évaluation afin que l'organisme de certification puisse assurer que les résultats de l'évaluation correspondent à la cible d'évaluation opérationnelle (in fine).*** Le travail des évaluateurs devrait être régi par un système de contrôle de la qualité qui recherche la conformité à la norme [EN45] afin que les fournitures d'évaluation puissent être contrôlées et gérées conformément aux souhaits du commanditaire et au schéma national.

Enlèvement des fournitures de l'évaluation

4.3.21 ***Les évaluateurs doivent faire enlever toutes les fournitures de l'évaluation une fois l'évaluation terminée (à l'issue de la phase Conclusion). Pour ce faire, l'une ou plusieurs des solutions suivantes sont envisageables :***

a) ***destruction des fournitures ;***

b) ***restitution des fournitures ;***

c) ***archivage des fournitures.***

4.3.22 ***Tout matériel archivé doit être conservé conformément aux exigences du schéma national.***

4.3.23 Les règles d'enlèvenent des fournitures d'évaluation devraient être déterminées d'un commun accord avec le commanditaire avant le commencement de la phase II (Conduite).

Réévaluation et réutilisation des fournitures

Généralités

4.3.24 Cette section fournit des conseils aux évaluateurs sur les données requises pour les évaluations pour lesquelles des résultats d'évaluations précédentes font partie des données disponibles. Le chapitre 4.6 décrit comment ces évaluations sont effectuées.

4.3.25 **Une réévaluation** d'une cible d'évaluation peut être effectuée lorsque la cible d'évaluation ou les fournitures de l'évaluation qui lui sont associées changent. Les exemples de changements comprennent l'augmentation du niveau d'évaluation visé de la cible d'évaluation ou l'ajout à sa cible de sécurité de fonctions dédiées à la sécurité. Le commanditaire réalise une estimation de l'impact des changements et détermine la ligne d'action appropriée afin que les résultats de l'évaluation précédente puissent être ré-affirmés conformément aux conseils qui figurent dans l'annexe 6.D de la partie 6.

4.3.26 **La réutilisation** des résultats d'évaluation est une technique qui permet de diminuer l'effort d'évaluation d'une cible d'évaluation qui comprend une ou plusieurs cibles d'évaluation précédemment évaluées. Les résultats de l'évaluation d'origine peuvent demeurer ou cesser d'être valides en fonction du contexte de l'évaluation de la nouvelle cible d'évaluation.

4.3.27 Si le(s) niveau(x) d'évaluation du/des composant(s) évalué(s) précédemment est supérieur ou égal au niveau d'évaluation visé de la cible d'évaluation, alors les résultats de conformité précédents sont confirmés par les certificats/rapports de certification.

4.3.28 Lorsqu'un produit ou un système certifié est utilisé comme composant d'une nouvelle cible d'évaluation, le contexte dans lequel il est utilisé aura changé. C'est pourquoi, bien que la conformité du composant certifié par rapport à sa cible de sécurité originale soit encore valide, son efficacité par rapport à la nouvelle cible de sécurité dans le contexte de sa nouvelle utilisation doit être ré-affirmée.

4.3.29 Par conséquent, on s'attendra à ce que le commanditaire livre les fournitures de la nouvelle cible d'évaluation pour le niveau d'évaluation visé, accompagnées des certificats/rapports de certification pour tous les composants certifiés.

4.3.30 Cependant, les fournitures relatives à la conformité pour ces composants de la cible d'évaluation peuvent être exigées pour soutenir l'analyse de l'efficacité.

4.3.31 Les fournitures relatives à l'efficacité de la nouvelle cible d'évaluation devront couvrir l'efficacité du/des produit(s) déjà évalué(s) en fonction de leur utilisation dans leur nouveau contexte. Par exemple, il faudra avoir démontré que la cible de sécurité pour la nouvelle cible d'évaluation a fait un usage pertinent des produits déja évalués. De la même façon, la cohésion entre *tous* les composants de la nouvelle cible d'évaluation devra être traitée par le commanditaire, y compris quand certains de ces composants disposent de certificats/rapports de certification qui proviennent de leur(s) évaluation(s) originale(s).

Disponibilité des résultats de la certification et de l'évaluation

4.3.32 Le certificat/rapport de certification ou le RTE (ou une partie de celui-ci) pourrait servir de donnée pour la réévaluation ou pour la réutilisation. En pratique, la mesure dans laquelle sont disponibles les résultats des évaluations précédentes est déterminée suivant que ces évaluations ont été conduites :

a) par le même CESTI ;

b) par un CESTI différent dans le cadre du même schéma national ;

c) par un CESTI dans le cadre d'un schéma national différent.

4.3.33 Le RTE peut contenir des informations sensibles sur le plan commercial et national qui ne devraient pas être communiquées au grand public. Le RTE ne peut donc être mis qu'à la disposition des CESTI qui travaillent dans le cadre d'un schéma national particulier. De plus, les informations liées à la réévaluation sont facultatives et peuvent ne pas toujours exister dans le RTE.

4.3.34 Le certificat/rapport de certification sera accessible au public et fournira un résumé de la cible d'évaluation et de son évaluation (voir la partie 2 de l'ITSEM). Les commanditaires seront donc toujours en mesure de fournir les certificats/rapports de certification aux CESTI.

4.3.35 En ce qui concerne la disponibilité des résultats de l'évaluation, les règles des schémas nationaux seront appliquées dans tous les cas.

Chapitre 4.4 Conduite de l'évaluation

Introduction

4.4.1 Le présent chapitre fonde le processus d'évaluation qui est recommandé pour toutes les évaluations selon les critères ITSEC, et énonce certaines exigences à caractère obligatoire. Les aspects procéduraux de l'organisation de ce processus (par exemple, les procédures détaillées à suivre pour **rendre compte des problèmes** tout au long des évaluations) ne sont pas rendus obligatoires dans ce chapitre. Ces aspects sont laissés à la discrétion des schémas nationaux.

4.4.2 Le processus d'évaluation est conçu pour être en conformité avec la philosophie et avec les principes établis dans la partie 3 de l'ITSEM. Le processus porte sur la façon de planifier, de réaliser et de rendre compte de l'évaluation de sorte qu'il soit aisé d'en démontrer la conformité avec les ITSEC et l'ITSEM.

4.4.3 Les travaux techniques réalisés sont débattus dans les sections suivantes intitulées *Programmes de travail*, *Application des ITSEC*, et dans le chapitre 4.5.

Programmes de travail

Généralités

4.4.4 ***Pour qu'une cible d'évaluation soit certifiée, son évaluation doit être conduite en conformité avec les critères ITSEC et l'ITSEM et avec les exigences des schémas nationaux.***

4.4.5 Une évaluation est menée à bien en accomplissant chacune des tâches spécifiées par les ITSEC. Afin de décrire la structure d'une évaluation et les relations qui existent entre les tâches de l'évaluateur, le concept d'un PTE (Plan de Travail d'Évaluation)générique est introduit dans cette section.

4.4.6 Un PTE générique décrit l'organisation des travaux requis pour les évaluations ; en d'autres termes, il s'agit d'une description des tâches impliquées dans une évaluation et de leurs relations.

4.4.7 Un PTE générique est conçu pour être appliquable à l'évaluation d'une grande variété de systèmes et de produits. Il est également conçu pour être généralement applicable à tous les niveaux d'évaluation. De nombreux PTE appliquables de manière générale sont concevables ; certains seront plus efficaces et plus flexibles que d'autres, mais tous sont susceptibles de mettre en oeuvre des interprétations valides des critères ITSEC.

4.4.8 Le PTE générique exprime simplement la façon dont une évaluation devrait être menée à terme conformément à la philosophie et aux principes d'évaluation de la partie 3 de l'ITSEM.

4.4.9 Les fournitures requises sont répertoriées dans l'annexe 6.A de la partie 6. Cette section traite de l'évaluation de ces fournitures. Pour évaluer selon les critères ITSEC, il faut :

a) vérifier que les fournitures sont conformes aux exigences des ITSEC ;

b) vérifier que les spécifications de sécurité, qui sont décrites dans la cible de sécurité, sont réalisées de manière adéquate ;

c) vérifier qu'aucune **vulnérabilité exploitable** n'existe dans la cible d'évaluation opérationnelle.

4.4.10 Les actions ci-dessus peuvent être résumées par l'expression suivante "Effectuer toutes les tâches relatives à l'efficacité et à la conformité spécifiées dans les critères ITSEC". Cependant, il est impossible de débattre de chaque tâche de l'évaluateur à un niveau aussi générique étant donné qu'une grande diversité de cibles d'évaluation peut devoir être évaluée à n'importe quel niveau d'évaluation. C'est pourquoi le concept d'activité est introduit de manière à pouvoir traiter le processus d'évaluation sur le plan générique.

4.4.11 Il est important d'être conscient de la distinction entre *tâches* et *activités*. Une *tâche* est une tâche de l'évaluateur qui figure dans les critères ITSEC. Une *activité* est un groupe générique de tâches qui poursuit un objectif spécifique, tel que l'attribution d'un verdict à une **représentation** particulière.

Activités génériques d'évaluation

4.4.12 La liste suivante (non triée) identifie les noms des activités génériques d'évaluation qui seront exécutées lors de la phase d'évaluation. Les numéros de paragraphe des ITSEC apparaissent entre accolades {} ; *n* peut être n'importe quel nombre compris entre 1 et 6 :

Vérifier l'**analyse de pertinence**{3.16}
Vérifier l'**analyse de cohésion**{3.20}
Examiner la résistance des mécanismes{3.24}
Examiner les **vulnérabilités de construction**{3.28}
Examiner la facilité d'emploi{3.33}
Examiner les **vulnérabilités en exploitation**{3.37}
Vérifier les spécifications des besoins{En.4}
Vérifier la conception générale{En.7}
Vérifier la conception détaillée{En.10}
Vérifier la réalisation{En.13}
Vérifier l'environnement de développement{En.17, En.20, En.23}
Vérifier la documentation d'exploitation{En.27,En.30}
Vérifier l'environnement d'exploitation{En.34,En.37}
Exécuter les tests de pénétration{3.24, 3.28, 3.33, 3.37}
Rédiger les rapports{5.11}

4.4.13 A l'exception de l'activité *Exécution des tests de pénétration*, les activités techniques d'évaluation correspondent à l'application des critères d'efficacité et de conformité, tels qu'ils apparaissent dans les ITSEC.

4.4.14 En ce qui concerne les noms des activités, la seule distinction entre *Vérification* et *Examen* est que la *vérification* implique principalement l'analyse des fournitures alors que l'*examen* fournit également des données pour les tests de pénétration. Les tests de pénétration sont explicitement liés à ces activités, mais ont été affectés à une activité distincte pour deux raisons :

a) pour souligner que les analyses précédentes sont consolidées et que les tests sont conçus pendant cette activité ;

b) pour indiquer que de grands ensembles de tests effectifs sont normalement exécutés ensemble.

4.4.15 L'activité *Vérifier l'analyse de pertinence* exige des évaluateurs qu'ils vérifient l'analyse de pertinence du développeur. Cela peut mettre en évidence des vulnérabilités dues à la raison suivante : une fonction dédiée à la sécurité ne parvient pas à atteindre un objectif de sécurité pour une menace identifiée dans la cible de sécurité.

4.4.16 L'activité *Vérifier l'analyse de cohésion* exige des évaluateurs qu'ils examinent l'analyse de cohésion du développeur et établissent si l'ensemble des fonctions dédiées à la sécurité, considérées comme un tout, satisfait convenablement tous les objectifs de sécurité.

4.4.17 L'activité *Examiner la résistance des mécanismes* exige des évaluateurs qu'ils identifient les mécanismes qui n'atteignent pas la résistance minimum des mécanismes requise par la cible de sécurité. La résistance des mécanismes est abordée dans l'annexe 6.C de la partie 6.

4.4.18 Au cours de l'évaluation de la conformité, les évaluateurs améliorent leur compréhension de la cible d'évaluation, compréhension qu'ils utilisent au cours de l'activité *Examiner les vulnérabilités de construction* afin d'essayer d'identifier des vulnérabilités dans la construction de la cible d'évaluation.

4.4.19 Les erreurs décelées lors de l'évaluation de la conformité sont une source de vulnérabilités de construction. Cependant, il est possible qu'un composant soit tenu pour correct (dans le sens de **raffinement correct**), alors qu'il contient encore des vulnérabilités. Ceci parce que :

a) au fur et à mesure que le processus de raffinement progresse, de nouvelles fonctionnalités sont ajoutées ;

b) les techniques de vérification du raffinement habituelles ne détecteront pas certaines vulnérabilités, telles que les canaux cachés.

4.4.20 Par conséquent cette activité demande des évaluateurs qu'ils examinent les erreurs de raffinement, ainsi que les fonctionnalités supplémentaires introduites lors de chaque phase de développement, à la recherche de vulnérabilités exploitables.

4.4.21 L'activité *Examiner la facilité d'emploi* exige des évaluateurs qu'ils examinent les modes d'exploitation non sûrs de la cible d'évaluation. Par conséquent, cette activité est étroitement liée aux autres activités relatives à l'exploitation.

4.4.22 L'activité *Examiner des vulnérabilités en exploitation* exige des évaluateurs qu'ils examinent l'exploitation de la cible d'évaluation. Les évaluateurs s'efforcent d'identifier des vulnérabilités dans la manière dont la cible d'évaluation est utilisée.

4.4.23 Les vulnérabilités en exploitation concernent la frontière entre les **contre-mesures** TI et non TI, telles que les procédures opérationnelles qui portent sur la sécurité physique, la gestion non électronique de clefs et la distribution de badges de sécurité. Les évaluateurs seront concernés par les contre-mesures non TI si une des conditions suivantes est remplie :

a) elles apparaissent comme un élément de la documentation d'exploitation ;

b) la cible de sécurité est formulée sur la base d'une politique de sécurité d'un système (voir les paragraphes 2.8 à 2.15 des ITSEC) ;

c) elles apparaissent comme un élément de l'argumentaire du produit.

4.4.24 Les contre-mesures non TI interviennent généralement lorsque les vulnérabilités de construction nécessitent des contre-mesures non TI pour préserver la sécurité d'une cible d'évaluation. Par conséquent, lors de l'évaluation des vulnérabilités en exploitation, les évaluateurs sont principalement soucieux de s'assurer que les contre-mesures non TI contrent effectivement les vulnérabilités de construction identifiées.

4.4.25 L'activité *Vérifier les spécifications des besoins* exige des évaluateurs qu'ils assurent que la cible de sécurité définit convenablement les fonctions dédiées à la sécurité et qu'elle n'est pas contradictoire. La cible de sécurité devrait identifier clairement les fonctions dédiées à la sécurité, le niveau d'évaluation visé, la cotation de la résistance des mécanismes et les mesures externes de sécurité à prendre en compte au cours de l'évaluation.

4.4.26 La première étape de développement, depuis les spécifications des besoins jusqu'à la conception générale, est d'une importance particulière car elle fournit l'affectation de plus haut niveau des fonctions abstraites aux composants physiques et logiques. Une tâche d'estimation importante pour les évaluateurs, exécutée lors de l'activité *Vérifier la conception générale*, est de décider si la séparation entre la fonctionnalité dédiée à la sécurité et celle non dédiée à la sécurité est "claire et efficace", car cela *permet à l'effort d'évaluation de se concentrer sur les secteurs limités de la TOE qui contribuent à la sécurité, et de suivre facilement la réalisation de la cible de sécurité, à mesure que la conception s'affine pour rentrer de plus en plus dans les détails*. (Extrait du paragraphe 4.20 des ITSEC.)

4.4.27 L'activité *Vérifier la conception détaillée* exige des évaluateurs qu'ils assurent que la politique de séparation est suivie et que les composants dédiés à la sécurité ont été correctement réalisés. Il peut exister plusieurs niveaux de conception détaillée.

4.4.28 Des remarques analogues à celles du dernier paragraphe s'appliquent à l'estimation de la réalisation à l'aide de l'activité *Vérifier la réalisation*. La différence se situe simplement dans le détail d'élaboration des composants élémentaires et des unités fonctionnelles identifiées au cours des dernières étapes de la conception détaillée (les tests fonctionnels deviennent alors possibles).

4.4.29 L'activité *Vérifier l'environnement du développement* exige des évaluateurs qu'ils vérifient les normes de développement, et plus particulièrement celles qui concernent les langages à utiliser à diverses étapes du développement. Les évaluateurs doivent avoir confiance dans le fait que la cible d'évaluation évaluée correspond à la cible d'évaluation développée, et que les notations utilisées pour la réalisation ne sont pas ambiguës. Cette activité concerne, par conséquent :

a) la gestion de configuration ;

b) les langages de programmation et compilateurs ;

c) la sécurité des développeurs.

4.4.30 L'activité *Vérifier la documentation d'exploitation* exige des évaluateurs qu'ils vérifient que la cible d'évaluation peut être administrée et utilisée conformément à ses objectifs de sécurité.

4.4.31 L'activité *Vérifier l'environnement d'exploitation* exige des évaluateurs qu'ils vérifient que la livraison de la cible d'évaluation est correctement effectuée, en montrant que la cible d'évaluation opérationnelle est une copie fidèle de la cible d'évaluation de l'environnement de développement et qu'elle peut être générée et utilisée conformément à ses objectifs de sécurité.

4.4.32 L'activité *Exécuter des tests de pénétration* exige des évaluateurs qu'ils regroupent les tâches "Effectuer des tests de pénétration" des ITSEC (par exemple, ceux qui sont effectués lors de l'activité *Examiner les vulnérabilités de construction*), toujours pour estimer l'efficacité et toujours dans le même but : déterminer si des vulnérabilités potentielles peuvent être exploitées dans la pratique.

4.4.33 L'activité *Rédiger des rapports* est introduite car les résultats de l'évaluation doivent être enregistrés. Les évaluateurs rédigent un RTE satisfaisant aux exigences du chapitre 4.7.

4.4.34 La figure 4.4.1 présente l'ensemble des tâches des ITSEC ainsi que l'activité à laquelle elles se rapportent. Dans la figure, *vérifier* * inclut toutes les tâches de vérification appropriées que les évaluateurs doivent effectuer selon les ITSEC. Les autres tâches sont présentées dans leur intégralité.

Figure 4.4.1 Les activités et leurs tâches de l'évaluateur (ITSEC) associées

Activité	Tâche
Vérifier l'analyse de pertinence	Vérifier*
Vérifier l'analyse de cohésion	Vérifier*
Examiner la résistance des mécanismes	Vérifier*
Examiner les vulnérabilités de construction	Vérifier*, effectuer une analyse indépendante de vulnérabilité, en prenant en compte à la fois les vulnérabilités de construction énumérées et toute autre découverte pendant l'évaluation.
Examiner la facilité d'emploi	Vérifier*, exécuter à nouveau toutes les procédures de configuration et d'installation pour vérifier que la TOE peut être configurée et utilisée de façon sûre, en ayant pour seul guide la documentation de l'utilisateur et celle de l'administrateur.
Examiner les vulnérabilités en exploitation	Vérifier*, effectuer une analyse de vulnérabilité indépendante, en prenant en compte à la fois les vulnérabilités en exploitation énumérées et toute autre découverte pendant l'évaluation.
Vérifier les spécifications des besoins	Vérifier*
Vérifier la conception générale	Vérifier*
Vérifier la conception détaillée	Vérifier*
Vérifier la réalisation	Vérifier*, utiliser la bibliothèque des programmes de test pour vérifier certains résultats. Réaliser des tests complémentaires pour rechercher des erreurs. Enquêter sur toute présomption d'incohérence entre le code source et l'exécutable survenue durant le test, en utilisant les outils fournis par le commanditaire.
Vérifier l'environnement de développement Gestion de configuration Langages de programmation et compilateurs Sécurité des développeurs	 Vérifier*, utiliser les outils des développeurs pour régénérer des parties choisies de la cible d'évaluation et les comparer à la version soumise à l'évaluation. Vérifier*. Vérifier *, rechercher des erreurs dans les procédures
Vérifier la documentation d'exploitation	Vérifier*.
Vérifier l'environnement d'exploitation Livraison et configuration Démarrage et exploitation	 Vérifier*. Rechercher des erreurs dans les procédures de génération système Vérifier*, Rechercher des erreurs dans les procédures.
Exécuter les tests de pénétration	(Résistance des mécanismes) Effectuer des tests de pénétration au besoin pour confirmer ou infirmer la résistance minimum des mécanismes annoncée. (Vulnérabilités de construction) Effectuer des tests de pénétration pour confirmer ou infirmer que les vulnérabilités connues sont réellement exploitables en pratique. (Facilité d'emploi) Effectuer d'autres tests lorsque c'est nécessaire pour confirmer ou infirmer l'analyse de la facilité d'emploi. (Vulnérabilités en exploitation) Effectuer des tests de pénétration pour confirmer ou infirmer que les vulnérabilités connues sont réellement exploitables en pratique.

Programme générique de travail pour l'évaluation

4.4.35 Les ITSEC introduisent une mise en séquence implicite des activités en indiquant, par exemple, que la conformité et l'efficacité sont mélées. Cependant, cet ordre a besoin d'être explicité.

4.4.36 La notion de résultat intermédiaire est introduite pour représenter toute information produite par les évaluateurs au cours d'une activité et utilisée au cours d'une autre. Un résultat intermédiaire peut être dérivé ou copié des fournitures, mais n'est utilisé que par les évaluateurs dans l'accomplissement de leurs tâches. Ces résultats intermédiaires devraient faire l'objet d'enregistrements afin de faciliter la **répétabilité** et une réévaluation ultérieure. Les résultats intermédiaires peuvent permettre de déduire des dépendances génériques entre activités d'évaluation et, par conséquent, d'établir un programme des activités pertinentes.

4.4.37 Certains résultats intermédiaires sont directement dérivés des fournitures. Ce sont :

a) les menaces identifiées dans la cible de sécurité ;

b) les mesures externes de sécurité identifiées dans la cible de sécurité ;

c) les fonctions dédiées à la sécurité identifiées dans la cible de sécurité ;

d) les événements concernant la sécurité identifiés à partir des spécifications des besoins ;

e) les composants de la conception générale (et leurs types : dédiés à la sécurité, touchant à la sécurité, ou autres) ;

f) les fonctions touchant à la sécurité identifiées dans la conception ;

g) les mécanismes de sécurité identifiés dans les fournitures ;

h) les fonctions d'administration de la sécurité identifiées dans la documentation d'exploitation ;

i) les mécanismes critiques de sécurité identifiés dans l'analyse de la résistance des mécanismes.

4.4.38 D'autres résultats intermédiaires proviennent des travaux supplémentaires effectués par les évaluateurs :

a) les vulnérabilités potentielles de construction identifiées par les évaluateurs ;

b) les vulnérabilités potentielles en exploitation identifiées par les évaluateurs ;

c) les erreurs identifiées par les évaluateurs ;

d) les tests de pénétration définis par les évaluateurs ;

e) les vulnérabilités exploitables identifiées par les évaluateurs.

4.4.39 Finalement, le RTE rédigé au cours de l'évaluation est un résultat.

4.4.40 La figure 4.4.2 représente un tableau des activités d'évaluation et des produits de l'évaluation. Les produits de l'évaluation sont soit un résultat d'activité (représentée par un 'R'), soit une donnée d'activité (représentée par un 'D') à utiliser au cours de cette activité. Le résultat d'une activité peut être un produit complet ou une contribution à un produit d'évaluation qui résulte d'une autre activité. Par exemple, plusieurs activités liées à l'efficacité contribuent à la liste des vulnérabilités de construction établie par les évaluateurs, et cette liste fournit des données pour les tests de pénétration.

4.4.41 Les activités d'évaluation ne concernent donc pas seulement les fournitures pertinentes du développeur, mais également les produits d'évaluation. Par exemple, l'activité "Examiner les vulnérabilités de construction" exige des évaluateurs qu'ils examinent le résultat de l'activité "Examiner la résistance des mécanismes" ainsi que la liste des vulnérabilités de construction connues établie par le développeur.

4.4.42 Les dépendances de séquencement sont identifiées par l'application des règles suivantes :

a) toutes les activités qui ont pour résultat un produit de l'évaluation ou y contribuent doivent être terminées avant que toute autre activité utilisant ce produit de l'évaluation, elle, ne puisse être terminée.

b) pour qu'une activité soit terminée, tous les produits de l'évaluation pertinents doivent avoir été pris en compte (cela n'empêche pas d'effectuer partiellement des activités pour les achever par la suite ; par exemple, un sous-ensemble de FDS et de composants peut subir les tests de pénétration avant que d'autres FDS n'aient été vérifiées au niveau de la réalisation).

4.4.43 Par exemple, l'activité "Exécution des tests de pénétration" ne peut pas être terminée avant la fin de l'activité "Vérifier l'analyse de pertinence" (voir la figure 4.4.3). Cela est dû au fait que l'activité "Vérifier l'analyse de pertinence" peut identifier des vulnérabilités de construction que les évaluateurs doivent prendre en considération au cours de l'activité "Examiner les vulnérabilités de construction". La liste des vulnérabilités de construction établie par les évaluateurs sera alors utilisée pour identifier les tests de pénétration effectués dans le cadre de l'activité "Exécution des tests de pénétration" afin de constater si les vulnérabilités sont exploitables ou non.

4.4.44 A l'aide des dépendances identifiées dans la figure 4.4.2 et des règles (a) et (b) énoncées précédemment, on peut construire une séquence type selon laquelle seront achevées les activités (voir la figure 4.4.4).

4.4.45 La figure 4.4.4 représente donc un "PTE générique".

Figure 4.4.2 Dépendances entre les activités

Activités / Résultats intermédiaires	Menaces	Mesures de sécurité externes	FDS	Événements touchant à la sécurité	Composants (élémentaires compris)	Mécanismes de sécurité	Fonctions d'admin. sécurité	Mécanismes de sécurité critiques	Vuln. de construc.	FTS	Vuln. en exploit.	Erreurs	Tests de Pénétration	Vuln. exploitables	RTE
Spéc. des besoins	DR	DR	DR	DR		R					R	R			
Conception générale		D	D	R	DR					R		R			
Conception détaillée			D	R	DR	R		R		R		R			
Réalisation			D	R	DR	D						R			
Environnement de développement	D*				D							R			
Documentation d'exploitation			D	D	D		DR					R			
Environnement d'exploitation			D		D							R			
Pertinence	D	D	D			D			R						
Cohésion			D			D			R						
Résistance des mécanismes						D		DR	R				R		
Vulnérabilités de construction	D	D	D			D		D	D	D			R		
Facilité d'emploi	D	D	D	D			D				R		R		
Vulnérabilités en Exploitation	D	D	D			D		D			D		R		
Tests de pénétration													D	R	
Rédaction du RTE	D	D	D		D	D		D	D	D	D	D	D	D	R

Légende : * signifie que les menaces pesant sur l'environnement de développement peuvent être ou ne pas être documentées dans la cible de sécurité
D (donnée) signifie qu'une activité nécessite un résultat intermédiaire
R (Résultat) signifie qu'une activité produit un résultat intermédiaire

FDS : Fonctions dédiées à la sécurité
FTS : Fonctions touchant à la sécurité

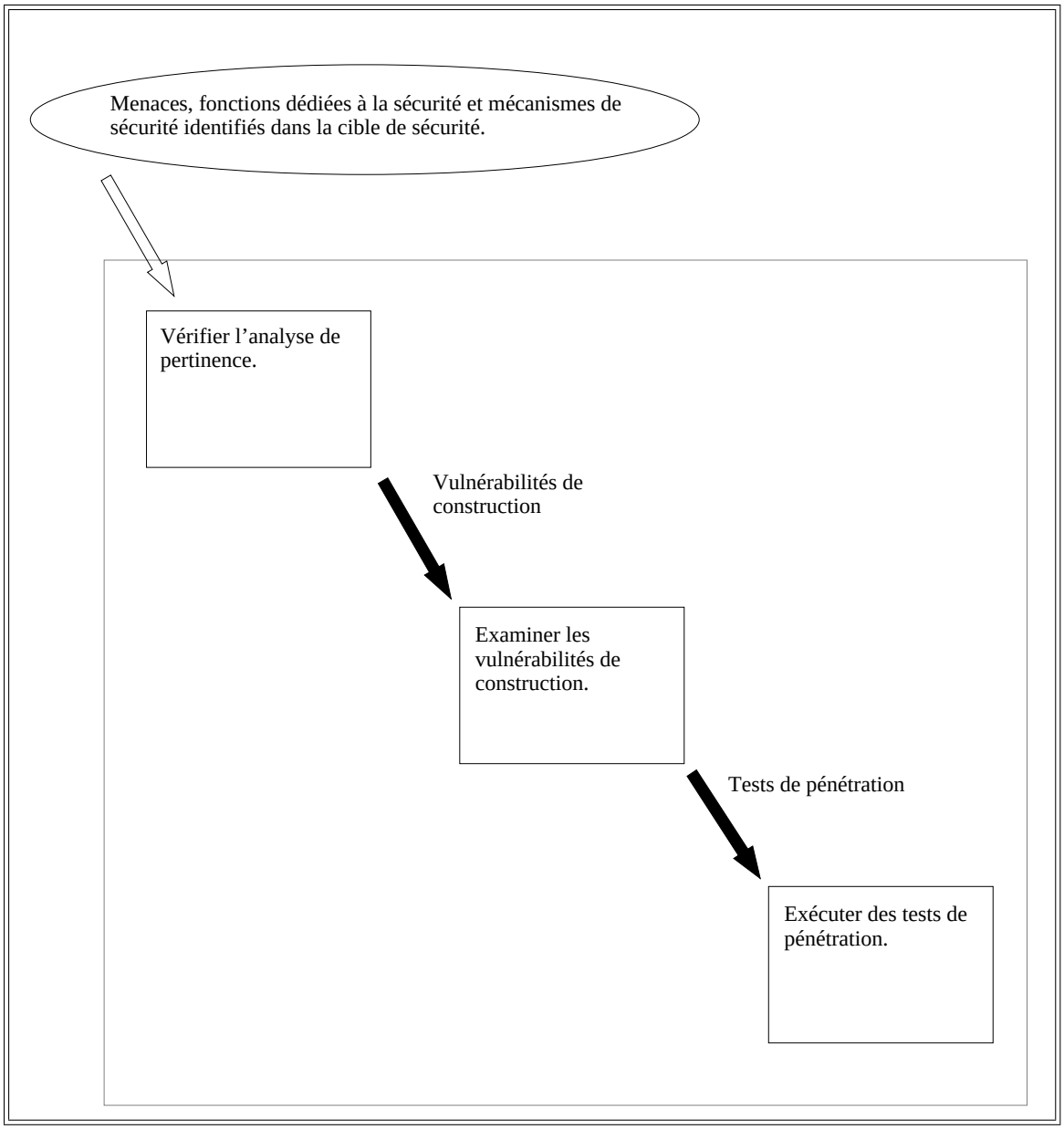


Figure 4.4.3 Exemple de dépendances des activités

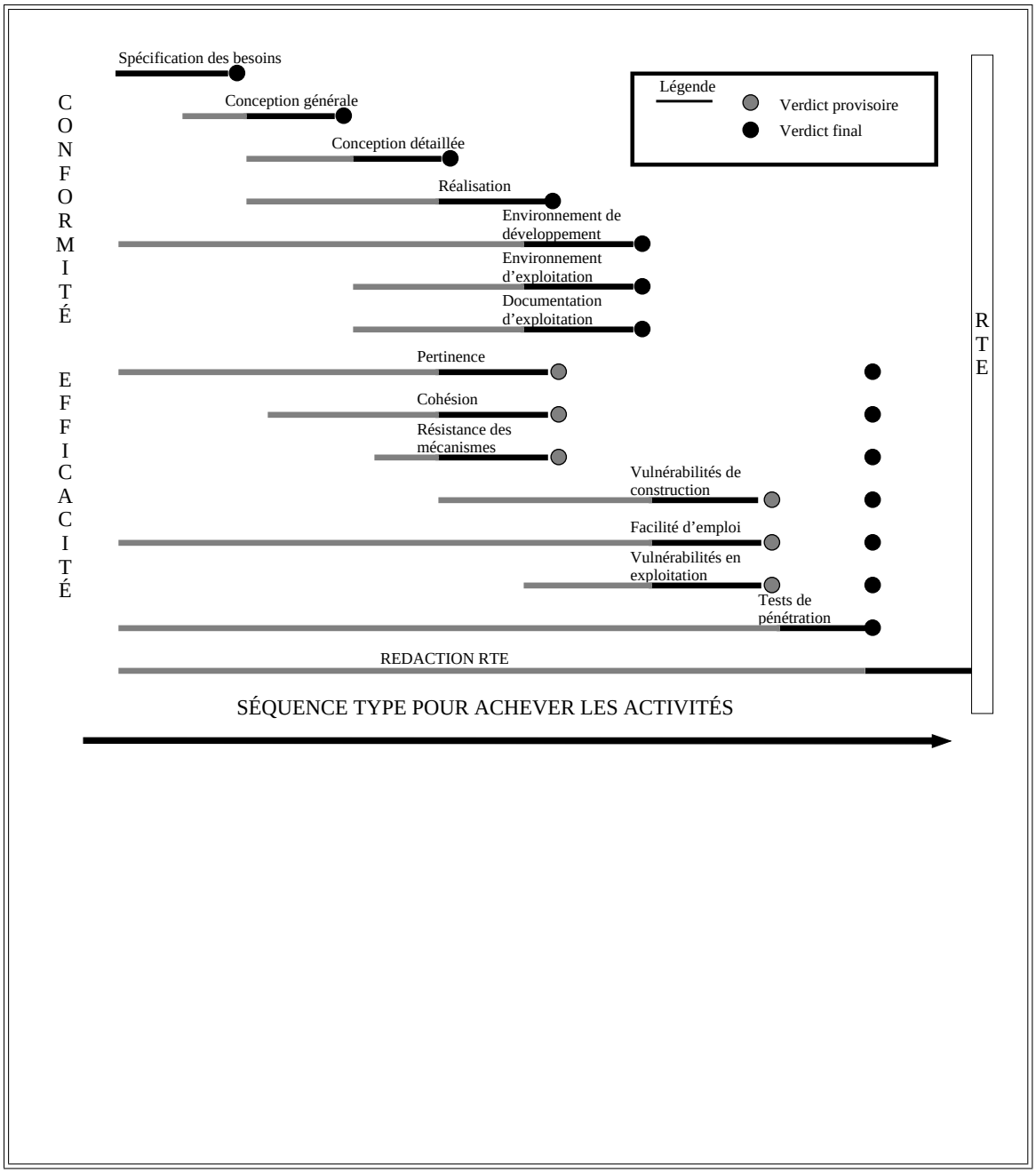


Figure 4.4.4 Un programme générique de travail pour l'évaluation

Construction des programmes de travail pour l'évaluation

4.4.46 Avant de commencer la conduite d'une évaluation, les évaluateurs devraient être conscients du travail exigé. Cela implique l'élaboration d'un programme pour le travail à réaliser, c'est-à-dire un PTE.

4.4.47 Afin de rendre plus facile la planification et l'enregistrement des travaux d'évaluation, il est nécessaire d'introduire le concept de lot. Le lot représente une unité de travail réalisée par les évaluateurs.

4.4.48 Une activité peut être divisée en plusieurs lots ou plusieurs activités peuvent être exécutées en un seul lot.

4.4.49 Lors du développement de PTE spécifiques à partir des PTE génériques susmentionnés, les caractéristiques spécifiques d'une évaluation devraient être incorporées dans son programme. Ces caractéristiques comprennent :

a) le niveau d'évaluation visé et la cotation minimum de la résistance des mécanismes ;

b) les noms spécifiques des fournitures ; par exemple, une référence à la partie précise d'un document ou de plusieurs documents, contenant la conception générale (voir l'annexe 6.A de la partie 6) ;

c) un ensemble spécifique de niveaux d'abstraction pour la conception détaillée ;

d) une mention indiquant s'il s'agit d'une réévaluation et si des composants certifiés de la cible d'évaluation existent (ce point est traité dans le chapitre 4.6) ;

e) une mention indiquant si la cible d'évaluation est un système ou un produit ;

f) les exigences portant sur le suivi, par exemple, des réunions externes ;

g) une liste des fournitures, établissant un programme de la mise à disposition des fournitures par le commanditaire ;

h) une mention indiquant si les informations qui concernent la réévaluation sont exigées dans le RTE.

4.4.50 Le niveau d'évaluation visé a des conséquences importantes. C'est le niveau d'évaluation qui détermine les fournitures exigées par les évaluateurs, le contenu des fournitures et le travail des évaluateurs pour évaluer ces fournitures.

4.4.51 Par exemple, les ITSEC ne demandent aucune analyse du code source pour les niveaux d'évaluation E1 et E2, et par conséquent, le commanditaire n'est pas obligé de fournir ce code aux évaluateurs (cela se justifie car certaines activités liées à la conformité ne seront pas exécutées à des niveaux d'évaluation faibles).

4.4.52 Pour l'évaluation d'un petit produit à un niveau d'évaluation visé faible, où la charge totale d'évaluation représente peut-être moins de la moitié d'un homme-an sur une durée de deux mois, il est préférable d'avoir un seul lot appelé *Examiner la conformité de la conception générale*, voire un seul lot appelé "Estimer la conception générale" regroupant cette activité avec *Effectuer l'analyse de cohésion.*

4.4.53 Par opposition, pour un grand système réparti au niveau E6, où la charge totale d'évaluation pourrait représenter plusieurs hommes-an, il ne serait pas déraisonnable d'avoir un seul lot pour la seule tâche de l'évaluateur appelée *Vérifier la validité des arguments formels*, puisque cela peut entraîner d'importantes vérifications des travaux liés aux méthodes formelles.

4.4.54 Un exemple de décomposition d'une activité en lots consisterait, pour l'évaluation d'un grand système, à réaliser l'activité *Exécuter les tests de pénétration* par des lots, tels que "Préparer et spécifier les tests de pénétration" et "Exécuter et exploiter les tests de pénétration".

4.4.55 Le lot "Préparer et spécifier les tests de pénétration" comprendrait les aspects administratifs (comme l'accès au site et la mise à disposition de bureaux ; voir l'annexe 6.A de la partie 6) et les aspects techniques relatifs à la définition d'une planification de tests de pénétration et de tests répondant aux exigences du schéma national.

4.4.56 Le lot "Exécuter et exploiter les tests de pénétration" impliquerait l'exécution physique des tests de pénétration documentés et l'enregistrement des résultats. Il pourrait aussi impliquer l'exploitation de tous les aspects liés aux vulnérabilités présumées dans les composants du système ou impliquer de tester à nouveau des composants corrigés à la suite des tests de pénétration précédents qui ont mis en évidence des vulnérabilités.

4.4.57 Selon que la cible d'évaluation est un système ou un produit, il en résulte des répercussions techniques (par exemple, la vérification de la cible de sécurité impliquera des travaux légèrement différents) et des répercussions sur la planification (par exemple, un système peut avoir plusieurs sites d'exploitation qui devraient être visités et les tests de pénétration ne peuvent être effectués sur ces sites que suivant un calendrier prédéfini).

4.4.58 Un produit peut être livré aux CESTI pour que les évaluateurs y aient aisément accès pour les tests de pénétration ; cependant, la configuration et l'environnement d'exploitation à évaluer devraient être émulés par les évaluateurs. Il est par conséquent important de définir une "configuration d'évaluation" pour l'évaluation d'un produit. Les évaluateurs et les commanditaires devraient se mettre d'accord sur cette définition. Elle doit être documentée dans le RTE (voir le chapitre 4.7).

4.4.59 Les résultats des tests de pénétration sont enregistrés dans le RTE comme cela est décrit dans le chapitre 4.7. Ils peuvent aussi être stockés dans une base de données d'évaluation locale. Le stockage des résultats de l'évaluation est laissé à la discrétion des schémas nationaux.

4.4.60 Lorsqu'un commanditaire s'attend à ce qu'une cible d'évaluation soit modifiée, mais qu'il souhaite maintenir le certificat/rapport de certification, il peut demander à ce que les évaluateurs joignent des informations pour **l'analyse d'impact** et pour la réévaluation dans le chapitre 7 facultatif du RTE. Cela devrait être pris en compte dans le PTE.

Application des critères ITSEC

Introduction

4.4.61 L'objectif de l'évaluation est d'élaborer des verdicts sur le respect des critères ITSEC par une cible d'évaluation. Le processus de certification produit également des verdicts : sur la conformité de l'évaluation aux ITSEC et à l'ITSEM, et comment la cible d'évaluation a satisfait le niveau ITSEC visé.

4.4.62 Cette section fournit des conseils aux évaluateurs sur l'application des critères ITSEC pour aboutir à des verdicts d'évaluation.

Verdicts de l'évaluateur

4.4.63 Un verdict est prononcé chaque fois que les évaluateurs achèvent une tâche d'évaluation consignée dans les critères ITSEC. Un verdict ne peut être que : *réussite, échec, à confirmer*. Par exemple, la tâche *Vérifier que les informations fournies satisfont à toutes les exigences concernant le contenu, la présentation et les éléments de preuve* peut conduire aux verdicts suivants :

a) *réussite*, si les informations fournies s'avèrent satisfaire toutes les exigences concernant le contenu, la présentation et les éléments de preuve.

b) *échec*, si une non conformité est mise en évidence dans laquelle les informations fournies ne satisfont pas tous les critères concernant le contenu, la présentation et les éléments de preuve.

c) *à confirmer*, si les évaluateurs n'ont pas pu prononcer un verdict de réussite ou d'échec. Ce verdict indique que la tâche de l'évaluateur n'est pas terminée car, par exemple, la tâche a été exécutée sur une fourniture provisoire, ou les évaluateurs ne pouvaient pas comprendre une partie des fournitures.

4.4.64 ***Si un verdict d'échec est prononcé, les évaluateurs doivent informer les organismes appropriés au moyen du mécanisme de rapport d'anomalie.*** Il est possible de se mettre d'accord avec le commanditaire sur une solution qui sera apportée à l'anomalie. Si l'anomalie est résolue, le verdict peut changer.

4.4.65 ***Tous les verdicts à confirmer devraient, par la suite, devenir des verdicts de réussite ou d'échec. Si un verdict à confirmer est prononcé, les évaluateurs doivent se mettre d'accord avec le commanditaire sur une procédure pour obtenir un verdict concluant.*** Cela peut entraîner l'attente d'une représentation ultérieure ; l'attente d'une version plus récente de la même représentation ; ou la tenue d'une réunion avec le développeur pour discuter des problèmes techniques impliqués. ***Si aucune solution n'est trouvée, alors un verdict d'échec doit être prononcé.***

4.4.66 ***Un verdict de conformité doit être attribué à une représentation du développement, par exemple, les spécifications des besoins ou la conception générale. Un verdict de réussite est attribué à une représentation si toutes les tâches de l'évaluateur ont conduit à un verdict de réussite. Un verdict d'échec est attribué à une représentation si une des tâches de l'évaluateur a conduit à un verdict d'échec. Un verdict à confirmer est attribué si les tâches de l'évaluateur n'ont pas produit de verdict d'échec, mais ont conduit à un ou plusieurs verdicts à confirmer.***

4.4.67 ***Un verdict d'efficacité doit être attribué à chacun des aspects de l'efficacité (par exemple, la facilité d'emploi ou la pertinence). Un verdict provisoire est obtenu à partir des tâches de l'évaluateur effectuées concernant un aspect, de la même façon que pour la conformité.***

4.4.68 A noter que chaque aspect de l'efficacité comprend une tâche de l'évaluateur *Vérifier que l'analyse a pris en compte toutes les informations données dans la figure 4 pour le niveau d'évaluation considéré*. La figure 4 des ITSEC indique que la représentation de l'exploitation doit être prise en compte pour tous les niveaux d'évaluation. Les tests de pénétration peuvent également révéler des vulnérabilités concernant tous les critères d'efficacité. ***Par conséquent, aucun verdict final d'efficacité ne peut être attribué avant la fin des tests de pénétration.***

4.4.69 Les estimations des vulnérabilités en exploitation et de construction exigent des évaluateurs qu'ils fassent des analyses indépendantes, en tenant compte des vulnérabilités découvertes au cours de l'évaluation. ***Cela implique que ces estimations ne peuvent pas être achevées avant la fin de l'évaluation de la conformité.***

4.4.70 Les dépendances entre les tâches de l'évaluateur sont traitées plus en détail dans la section précédente *Programme générique de travail pour l'évaluation*.

4.4.71 La conclusion finale d'une évaluation constitue le résultat pour la cible d'évaluation dans son ensemble. Tous les verdicts à confirmer devraient être résolus (et remplacés par réussite ou échec) pour arriver à la conclusion finale.

4.4.72 Il peut arriver qu'une cible d'évaluation ne réponde pas aux critères de conformité, mais soit tout de même satisfaisante pour un niveau d'évaluation inférieur, si ce niveau n'inclut pas les critères pour lesquels la cible d'évaluation a échoué. Dans ce cas, il est possible de recommander l'attribution d'un niveau inférieur. Si une cible d'évaluation ne peut atteindre la résistance des mécanismes annoncée, il est possible d'attribuer une résistance des mécanismes plus faible. ***Si une cible d'évaluation échoue selon l'un des autres aspects de l'efficacité, alors les évaluateurs doivent prononcer un verdict d'échec envers la cible d'évaluation.***

4.4.73 Le développeur peut accepter de modifier une cible d'évaluation avec un verdict d'échec ou des fournitures de l'évaluation, y compris la cible de sécurité. Si les modifications sont adéquates, un verdict d'échec peut être repris.

Chapitre 4.5 Techniques et Outils d'évaluation

Objectifs de cette section

4.5.1 L'équivalence technique des résultats d'évaluation repose sur l'utilisation de procédures normalisées, qui comprennent l'utilisation d'une technologie d'évaluation adaptée. Cela suppose l'utilisation d'outils et de techniques adaptés.

4.5.2 Dans le processus d'évaluation, les évaluateurs peuvent utiliser des outils et des techniques d'évaluation afin de réaliser le PTE avec le meilleur rapport coût/performance et avec les plus brefs délais. L'utilisation de ces techniques et outils aide à atteindre l'**objectivité**, la répétabilité et la **reproductibilité**. L'annexe 6.E de la partie 6 donne des avis d'ordre général aux développeurs d'outils d'évaluation.

4.5.3 L'objectif de cette section est de décrire à la fois des techniques élémentaires, telles que la revue de documents et la simulation, et les techniques et les outils qui peuvent être utilisés pour leur mise en oeuvre.

4.5.4 Les objectifs de cette section sont :

a) de traiter des techniques de base de l'évaluation ;

b) de débattre des questions concernant le choix et l'utilisation des outils pour l'évaluation ;

c) d'identifier et de décrire les différentes catégories de techniques et d'outils et d'indiquer la vraisemblable adéquation de chaque catégorie aux activités d'évaluation.

4.5.5 Il n'entre pas dans le champ d'application de l'ITSEM de recommander des techniques et des outils particuliers ; des normes nationales peuvent être appliquées et l'éventail des techniques et des outils applicables évolue continuellement. Cependant, cette section a été rédigée pour soutenir l'objectif d'équivalence technique des résultats d'évaluation.

4.5.6 Aucun exemple spécifique de technique ou d'outil n'est rendu obligatoire par souci de ne pas sembler avaliser un quelconque produit.

Techniques de base

Généralités

4.5.7 Cette section traite des techniques de base d'évaluation. Celles-ci peuvent être utilisées pour une grande variété de niveaux d'évaluation et de cibles d'évaluation.

Examen informel

4.5.8 La technique d'évaluation la plus élémentaire est l'examen informel de documents.

4.5.9 Cette technique peut être utilisée pour toutes les tâches de l'évaluateur *vérifier* et *rechercher* des ITSEC. Avec des représentations informelles ou non-informatiques, il n'y a que peu d'alternatives à cette méthode. Cette méthode comporte certains dangers et il est recommandé de suivre les conseils ci-dessous pour les contrer :

a) l'examen informel n'est pas adapté pour une personne qui travaille seule pendant de longues périodes car la qualité des résultats se dégradera. Dans la mesure du possible, deux évaluateurs devraient travailler ensemble.

b) ***Les évaluateurs qui réalisent un examen informel doivent produire des éléments de preuve documentés suffisants (par exemple, des résultats intermédiaires) pour permettre une estimation du travail effectué.***

Analyse de concordance

4.5.10 L'analyse de concordance est une technique un peu plus méthodique. Elle est utilisée pour vérifier la cohèrence entre deux représentations. Les étapes impliquées sont les suivantes :

a) pour chaque composant de la représentation de niveau supérieur, vérifier (à l'aide des preuves de traçabilité du développeur, lorsque cela est possible) qu'il est correctement réalisé dans la représentation de niveau inférieur.

b) Pour chaque composant de la représentation de niveau inférieur, vérifier que son existence est justifiée par la représentation de niveau supérieur.

4.5.11 A nouveau, les travaux sont susceptibles d'être en grande partie manuels et dans ce cas, les conseils susmentionnés s'appliquent. Dans certains cas, une base de données ou un système hypertexte peut être utile pour conserver une trace de la correspondance entre des représentations.

4.5.12 ***Les évaluateurs doivent être capables de démontrer qu'ils ont pris en considération toutes les parties pertinentes de la cible d'évaluation dans leur analyse.***

Analyse de traçabilité

4.5.13 L'analyse de traçabilité est l'un des principes sous-jacents de l'évaluation. L'analyse de traçabilité est utilisée pour décrire la notion de raffinement correct des fonctions dédiées à la sécurité à travers les représentations de la cible d'évaluation jusqu'à sa réalisation finale sous la forme de code exécutable et de circuits électroniques.

4.5.14 L'assurance dans la cible d'évaluation est construite par la vérification des évaluateurs que les fonctions dédiées à la sécurité de la cible de sécurité sont correctement raffinées tout au long de la conception générale, de la conception détaillée, de la réalisation et de l'exploitation de la cible d'évaluation. Par conséquent, l'assurance augmente progressivement au fur et à mesure que d'autres représentations de la cible d'évaluation sont vérifiées en termes de traçabilité (de ce fait, le nombre de représentations, et leur niveau de détail, augmente progressivement avec le niveau d'évaluation).

4.5.15 Une technique d'évaluation élémentaire consiste donc à tracer chaque fonction dédiée à la sécurité à travers les diverses représentations de la cible d'évaluation jusque et y compris dans l'exploitation de la cible d'évaluation.

4.5.16 Cela a été signalé dans la section précédente *Programme générique de travail pour l'évaluation* par le nombre important des résultats intermédiaires concernant la traçabilité.

Le processus de revue

4.5.17 Le processus d'évaluation implique un nombre considérable d'analyses informelles. Il est important de pouvoir démontrer que ces analyses ont été réalisées objectivement. Une manière de faire est que chaque travail d'un évaluateur soit vérifié par d'autres. Ceci minimise les éléments subjectifs dans les résultats. *Le processus de revue* décrit ci-dessous est une des approches pour effectuer cette vérification, même si une réunion formelle peut ne pas être nécessaire.

4.5.18 ***Toutes les résultats de l'évaluation (voir le chapitre 4.7) doivent faire l'objet d'une revue.***

4.5.19 Le processus de revue devrait impliquer, au moins, les rôles suivants :

a) le chef de projet, qui est le responsable de la conduite technique de l'évaluation ;

b) l'auteur, le ou les évaluateurs qui ont effectué l'analyse ;

c) le modérateur, qui est responsable pour assurer de façon indépendante que la revue est correctement effectuée.

4.5.20 D'autres personnes peuvent être impliquées, par exemple, des spécialistes techniques, des représentants de l'organisme de certification ou d'autres évaluateurs (en particulier si l'auteur et le chef de projet sont la même personne).

4.5.21 Le processus de revue passe par un certain nombre de phases :

a) Lorsqu'un résultat de l'évaluation est achevé, le chef de projet fixe une date pour une réunion de revue qui convient à tous les participants. La date fixée doit permettre à tous les participants d'étudier de façon approfondie le résultat.

b) Avant la réunion, les participants étudient le résultat et y recherchent des erreurs.

c) Pendant la réunion, les participants débattent du résultat et de toute erreur découverte. Ils décident des modifications à apporter au résultat. En général, la réunion devrait porter principalement sur l'identification des modifications requises, plutôt que sur la nature exacte de ces modifications.

d) A la fin de la réunion, les participants décident si le résultat est acceptable tel quel, si des modifications mineures sont requises ou si des modifications majeures sont nécessaires, ces dernières devant faire l'objet d'une réunion de revue ultérieure.

e) La décision est enregistrée. Si les participants ne peuvent pas parvenir à un accord unanime, c'est la décision du chef de projet qui sera retenue. Les opinions divergentes devraient, toutefois, être enregistrées.

Transcription

4.5.22 La transcription, ou modélisation, correspond à la traduction d'une représentation en une autre notation. Par exemple, un schéma Z peut être animé en Prolog afin que les évaluateurs puissent comprendre toutes les subtilités de la représentation originale. L'acte de transcription est souvent au moins aussi utile aux évaluateurs en termes de compréhension, que le produit final.

Analyse des défaillances

4.5.23 Une cible d'évaluation qui a des exigences de disponibilité dans sa cible de sécurité sera soumise à un certain nombre de menaces qui portent sur les défaillances de la cible d'évaluation. Ces menaces peuvent être soit des tentatives hostiles externes pour réduire la disponibilité, soit des menaces accidentelles internes qui proviennent de la défaillance de la cible d'évaluation elle-même.

4.5.24 Les menaces externes envers la disponibilité peuvent être considérées, lors de l'estimation de l'efficacité, de la même façon que les menaces externes envers l'intégrité ou envers la confidentialité. Ces analyses portent sur la fonctionnalité de sécurité fournie pour contrer une attaque extérieure à la cible d'évaluation.

4.5.25 Les causes internes de la perte de disponibilité doivent être estimées à l'aide d'une technique qui analyse les modes de défaillances d'une cible d'évaluation. Cette technique est appelée "Analyse de Mode de Défaillances et de leurs Effets (AMDE)" et est utilisée dans le domaine de la sûreté de fonctionnement pour étudier la fiabilité des équipements et des systèmes. La technique AMDE est décrite en détail dans une norme militaire des États-Unis [MS1629A].

4.5.26 L'AMDE fournit une technique normalisée qui permet de considérer tous les modes de défaillances de la cible d'évaluation et de leurs effets sur la disponibilité de la cible d'évaluation, en tenant compte de toutes les dispositions compensatoires intégrées dans la cible d'évaluation pour contrer les effets des défaillances.

4.5.27 L'analyse identifie, pour chaque composant considéré :

a) sa fonction ;

b) ses modes et causes de défaillances ;

c) les effets des défaillances, pour chaque représentation ;

d) sa méthode de détection des défaillances ;

e) ses dispositions compensatoires ;

f) la gravité résultante.

4.5.28 Cette technique peut être utilisée par les évaluateurs pour estimer si la cible d'évaluation est munie de dispositions adéquates pour contrer les menaces envers sa disponibilité qui émanent de ses propres défaillances.

Exécution des activités d'évaluation

Généralités

4.5.29 La figure 4.4.1 indique toutes les activités à exécuter par les évaluateurs. Celles-ci sont décrites ci-dessous et des techniques pertinentes sont proposées. Cependant, les tâches de l'évaluateur ne sont pas toutes traitées dans le détail.

Vérifier l'analyse de pertinence

4.5.30 La technique principale pour cette activité est un examen informel.

Vérifier l'analyse de cohésion

4.5.31 La technique principale pour cette activité est un examen informel.

4.5.32 Il peut s'avérer nécessaire de rechercher des canaux cachés dans la cible d'évaluation, même si les canaux cachés ne sont pas mentionnés dans la cible de sécurité. Les techniques pour l'analyse des canaux cachés reposent, pour la plupart, sur la "Méthode de la matrice des ressources partagées" [SRMM]. Les évaluateurs peuvent trouver des outils d'analyse de code source et des outils d'opération sur les matrices particulièrement utiles pour appliquer cette méthode à une cible d'évaluation.

Examiner les vulnérabilités de construction

4.5.33 La technique principale pour vérifier l'analyse du développeur est un examen informel.

4.5.34 ***Les évaluateurs sont également tenus d'effectuer leur propre analyse, fondée sur les vulnérabilités découvertes au cours de l'évaluation. Cela implique qu'ils doivent tenir un registre des problèmes découverts lors de l'évaluation. Ce registre doit comprendre les rapports d'anomalie, ainsi que les erreurs mineures de conformité rapportées de façon moins formelle.***

4.5.35 L'analyse des évaluateurs devrait aborder les méthodes génériques suivantes, qui peuvent être utilisées pour exploiter une vulnérabilité :

a) modifier la séquence prédéfinie d'appel des composants ;

b) exécuter un composant supplémentaire ;

c) utiliser des interruptions ou des fonctions d'ordonnancement pour perturber le séquencement ;

d) lire, écrire ou modifier des données internes, directement ou indirectement ;

e) exécuter des données qui ne sont pas destinées à être exécutées ou les rendre exécutables ;

f) utiliser un composant dans un contexte ou un but non prévu ;

g) générer des données non prévues pour un composant ;

h) activer la reprise après erreur ;

i) utiliser des détails de réalisation introduits dans les représentations de niveaux inférieurs ;

j) perturber le parallélisme ;

k) utiliser l'interaction entre des composants qui ne sont pas visibles à un niveau d'abstraction supérieur ;

l) invalider des hypothèses et des propriétés sur lesquelles reposent les composants de niveaux inférieurs ;

m) utiliser le délai entre la vérification et l'utilisation.

4.5.36 Les tâches de l'évaluateur qui concernent la conformité de l'exploitation peuvent révéler des vulnérabilités de construction ainsi que des vulnérabilités en exploitation. Par exemple, l'étude des commandes utilisateur décrites dans la documentation utilisateur peut révéler que l'objectif d'une contre-mesure est compromis si les commandes sont passées dans un ordre non prévu. Il s'agit plutôt d'une vulnérabilité de construction que d'une vulnérabilité en exploitation, car des propriétés de la cible d'évaluation introduites pendant sa construction en sont l'origine.

Examiner la résistance des mécanismes

4.5.37 Cette activité est effectuée principalement sous forme d'un examen informel.

4.5.38 Les mécanismes cryptographiques ne sont pas cotés par les CESTI (voir le paragraphe 3.23 des critères ITSEC).

4.5.39 L'annexe 6.C de la partie 6 débat à propos de la résistance des mécanismes.

Examiner la facilité d'emploi

4.5.40 Cette activité est exécutée principalement sous forme d'une analyse informelle.

4.5.41 Les évaluateurs sont tenus d'*exécuter à nouveau toutes les procédures de configuration pour vérifier que la TOE peut être configurée et utilisée de façon sûre, en n'utilisant comme guide que la documentation de l'utilisateur et la documentation d'administration*. Ceci nécessitera l'accès à la cible d'évaluation.

4.5.42 Pour un produit, il est peu probable que cet accès pose problème. Pour l'évaluation d'un système, cela peut s'avérer difficile car la cible d'évaluation peut déjà être configurée et installée et les évaluateurs peuvent ne pas être en mesure de répéter le processus. Dans ce cas, il est nécessaire de faire la distinction entre :

a) Les parties de l'installation et de la configuration qui ne sont effectuées qu'une seule fois. Dans ce cas, il suffit de vérifier que la configuration et l'installation de la cible d'évaluation ont été correctement faites. ***Si de telles parties d'une cible d'évaluation sont réinstallées ou reconfigurées, la cible d'évaluation doit être réévaluée.***

b) Les parties de l'installation et de la configuration qui peuvent être modifiées ultérieurement. ***Pour celles-ci, les évaluateurs doivent répéter les procédures d'installation et de configuration.*** Cependant, il n'est pas nécessaire de réévaluer ces parties, si elles sont réinstallées ou reconfigurées.

4.5.43 Les évaluateurs sont tenus d'*effectuer d'autres tests, quand c'est nécessaire pour confirmer ou infirmer l'analyse de la facilité d'emploi*. Ces tests peuvent faire partie de l'activité de test de pénétration.

Examiner les vulnérabilités en exploitation

4.5.44 Cet examen peut être réalisé en utilisant les mêmes techniques que pour *"Examiner les vulnérabilités de construction"*.

Vérifier les spécifications des besoins

4.5.45 La principale technique pour cette activité est un examen informel de la cible de sécurité.

4.5.46 A des niveaux d'évaluation supérieurs, les évaluateurs peuvent utiliser des outils d'animation pour examiner les parties complexes des cibles de sécurité.

4.5.47 Lors de l'estimation de l'adéquation des descriptions formelles à partir du niveau E4, les évaluateurs devraient se poser les questions suivantes :

a) La description formelle est-elle à un niveau d'abstraction acceptable, par exemple, est-il acceptable de décrire une porte logique en termes de logique classique (où la sortie de la porte est 0 ou 1) plutôt qu'en termes de logique ternaire (où la sortie de la porte peut être 0, 1 ou indéfinie) ?

b) La description formelle est-elle exprimée à l'aide d'une notation appropriée, par exemple, est-il acceptable d'utiliser, disons, Z plutôt que CSP pour décrire une cible d'évaluation qui est constituée d'un certain nombre de processus parallèles qui interragissent ?

c) L'omission de certaines parties de la cible de sécurité dans la description formelle est-elle justifiée, par exemple, du fait que cela dépasse l'état de l'art en matière de méthodes formelles ?

4.5.48 Les cibles de sécurité sont traitées dans l'annexe 6.B de la partie 6.

4.5.49 ***Si le commanditaire demande des informations pour la réévaluation dans le chapitre 7 du RTE, les évaluateurs doivent réunir les informations nécessaires au cours de cette activité.***

Vérifier la conception générale

4.5.50 Les principales techniques pour cette activité sont l'examen informel ou l'analyse informelle de concordance. A des niveaux d'évaluation supérieurs (c'est-à-dire à partir de E4), la modélisation peut être appropriée.

4.5.51 Au niveau d'évaluation E6, le développeur est tenu de prouver la cohérence entre l'expression formelle de la conception générale et le modèle formel de la politique de sécurité. Cela peut être évalué par un examen informel, ou il est peut-être possible d'utiliser des outils de vérification de preuve automatisés.

4.5.52 ***Si le commanditaire demande des informations pour la réévaluation dans le chapitre 7 du RTE, les évaluateurs doivent réunir les informations nécessaires au cours de cette activité.***

4.5.53 ***Lorsque les critères exigent que les descriptions soient exprimées à l'aide de notations semi-formelles ou formelles, les évaluateurs doivent vérifier que les notations utilisées et la façon dont elles sont utilisées sont appropriées. Pour ce faire, ils doivent comparer la notation avec les exigences des paragraphes 2.65 à 2.80 des ITSEC (Style de spécification).***

4.5.54 Par exemple, lorsqu'ils vérifient que la notation est acceptable en tant que notation formelle, les évaluateurs peuvent considérer les questions suivantes :

a) la notation est-elle une norme reconnue, ou est-elle académiquement reconnue (par exemple, Z, CSP, VDM et HOL) ?

b) la notation est-elle acceptable pour d'autres raisons pour l'organisme de certification ?

c) le commanditaire peut-il démontrer que la notation possède vraiment une syntaxe et une sémantique bien définies ?

4.5.55 ***Les évaluateurs doivent vérifier que le langage utilisé pour exprimer la conception générale permet d'exprimer les caractéristiques touchant à la sécurité.***

4.5.56 Par exemple, les modèles de données et les diagrammes de flot de données sont tous deux acceptés comme des notations semi-formelles. Cependant, une seule notation, telle qu'un modèle de données ou un diagramme de flot de données, peut ne pas permettre d'exprimer toutes les facettes de la conception générale d'une cible d'évaluation. Dans ce cas, le commanditaire pourrait utiliser plusieurs notations qui, combinées, fourniront une représentation complète de la conception générale.

Vérifier la conception détaillée

4.5.57 Les principales techniques pour cette activité sont un examen informel et une analyse informelle de concordance.

4.5.58 ***Lorsque une description semi-formelle de la conception est fournie aux évaluateurs, ils doivent vérifier que la description correspond au niveau de formalisme exigé par les critères ITSEC.*** Les styles semi-formels acceptables comprennent une représentation graphique (par exemple, des diagrammes de flot de données, des diagrammes de structure de processus) ou une utilisation restreinte clairement définie du langage naturel (voir les paragraphes 2.72 à 2.75 des ITSEC).

4.5.59 Par exemple, si le Langage de Description de Programmes (PDL) est fourni aux évaluateurs, alors ils pourraient s'assurer que le développeur dispose d'un ensemble défini de normes pour le PDL qui définissent clairement la syntaxe et la sémantique des structures de PDL.

4.5.60 Lorsqu'un développeur utilise des outils de génie logiciel (CASE), alors les évaluateurs devraient confirmer que la méthode sous-jacente imposée par l'outil est acceptable et conforme aux normes de qualité du développeur.

4.5.61 A partir du niveau E5, les ITSEC exigent que[1] *[la cible d'évaluation]... utilise de façon importante le découpage en couches, l'abstraction et la dissimulation des données.* Ces techniques sont bien connues dans les domaines où la sûreté est critique [ISO65A], et ont pour objectif d'aider à la compréhension et à la maintenance de la conception. Il faut remarquer que, puisque l'utilisation de ces techniques doit être importante plutôt qu'universelle, un seul cas de mise en défaut de ces techniques ne doit pas forcément conduire à un verdict négatif. ***Les évaluateurs doivent plutôt estimer si la conception de la cible d'évaluation leur semble claire.*** S'ils estiment que non, il est probable que le découpage en couches, l'abstraction et la dissimulation des données n'ont pas été utilisés de manière adéquate.

4.5.62 ***Les spécifications d'interface doivent faire l'objet d'une vérification de complétude et de validité par une vérification par recoupement du reste des spécifications de la fonctionnalité dédiée à la sécurité et touchant à la sécurité.***

4.5.63 ***Les variables communes, identifiées pour les niveaux E5 et E6, doivent être considérées comme une forme d'interface. Les évaluateurs doivent s'assurer qu'elles sont définies une seule fois et que l'utilisation de chaque variable commune par une unité fonctionnelle est justifiée et cohérente avec la définition de la variable commune.*** Une liste de contrôle, qui établit la correspondance entre les variables communes identifiées dans la conception détaillée et leurs références par unités fonctionnelles, doit être produite.

4.5.64 ***Si le commanditaire demande des informations pour la réévaluation dans le chapitre 7 du RTE, les évaluateurs doivent réunir les informations nécessaires au cours de cette activité.***

Vérifier la réalisation

4.5.65 Bien que cette activité ait plus de chances qu'une autre de bénéficier de l'utilisation d'outils automatisés, un examen informel et une analyse informelle de concordance peuvent encore être utilisés.

4.5.66 Si la réalisation comprend du code source, des outils d'analyse statique de code source peuvent être utilisés pour estimer la qualité du code et rechercher des types particuliers de vulnérabilités. Si la réalisation comprend des schémas descriptifs de matériel, les outils de CAO du développeur peuvent être utiles pour les analyser.

1. NdT : ITSEC E5.8:6, la traduction a été reprise.

4.5.67 Les évaluateurs sont tenus d'*utiliser la bibliothèque de programmes de tests pour vérifier par échantillonnage les résultats des tests*. Ceci constitue l'une des deux tâches de l'évaluateur qui autorisent l'échantillonnage. ***Les principes suivants doivent être suivis lors du choix de l'échantillon :***

a) ***L'échantillon doit fournir un échantillon de tests qui couvre une variété de composants, de fonctions dédiées et touchant à la sécurité, de sites du développeur (si plus d'un site est concerné) et de types de plates-formes informatiques (si plus d'une plate-forme est concernée).***

b) ***Le commanditaire et le développeur ne doivent pas être informés à l'avance de l'échantillon.***

c) ***La taille de l'échantillon considéré doit être acceptable pour l'organisme de certification.*** Afin de rendre le coût de l'évaluation prévisible, il est possible de fixer une taille d'échantillon avant le début de l'évaluation.

4.5.68 ***Lorsque l'échantillonnage est effectué, un argumentaire doit être fourni et l'échantillon utilisé doit être enregistré.***

4.5.69 Cette tâche peut exiger l'utilisation des systèmes de développement. Cela doit être pris en considération dans le contrat initial passé avec le commanditaire.

4.5.70 Les évaluateurs sont tenus (à partir du niveau E2) de *vérifier que les tests couvrent toutes les fonctions dédiées à la sécurité identifiées dans la cible de sécurité* [1]. ***Les évaluateurs doivent, au minimum, vérifier que pour chaque déclaration vérifiable de la cible de sécurité, au moins un test a été défini pour en faire sa démonstration.*** La justification donnée par le développeur (exigée à partir du niveau E4) à la question *pourquoi l'étendue de la couverture des tests est suffisante* peut fournir des informations utiles.

4.5.71 Les évaluateurs sont tenus (à partir du niveau E3) de *vérifier que les tests couvrent toutes les fonctions dédiées à la sécurité ou touchant à la sécurité identifiées dans la conception détaillée et tous les mécanismes de sécurité identifiables dans le code source ou les schémas descriptifs des matériels*. ***Pour la conception détaillée, les évaluateurs doivent vérifier que chaque interface de chaque composant élémentaire dédié ou touchant à la sécurité a été utilisée dans un test.*** Les évaluateurs peuvent vérifier cela à l'aide de la *correspondance faite par le développeur entre les tests et les fonctions dédiées à la sécurité et touchant à la sécurité définies dans la conception détaillée*.

4.5.72 Une couverture adéquate du code source a été atteinte si le commanditaire peut démontrer ce qui suit :

a) au niveau E3, chaque instruction du code source dédié à la sécurité a été testée ;

b) à partir du niveau E4, chaque instruction et branchement de tout le code source qui appartient à un composant élémentaire dédié à la sécurité ou touchant à la sécurité ont été testés.

1. NdT : ITSEC E2.13:3, la traduction a été reprise.

4.5.73 *Couverture du code source* : cet encadré explique le test des instructions et des branchements. Afin de tester chaque instruction du code source d'un programme séquentiel, le développeur doit exécuter chaque instruction du code source dans le programme au moins une fois. Afin de tester chaque instruction et branchement, le développeur doit exécuter chaque instruction du code source dans le programme au moins une fois et exécuter chaque structure de contrôle de toutes les façons possibles.

4.5.74 Il est plus facile de comprendre la signification de ces exigences à l'aide d'un exemple. Soit la séquence d'instructions suivante :

if a
then B;
else C;
endif;

if d
then E;
endif;

4.5.75 Afin de tester chaque instruction de ce programme, le développeur doit exécuter les instructions *B*, *C* et *E*, peut-être en exécutant le programme avec les conditions *a* et *d* vraies (exécution de B et de E), puis en répétant l'opération avec les conditions *a* fausse et *d* vraie (exécution de C et de E).

4.5.76 Afin de tester chaque instruction et branchement de ce programme, le développeur doit exécuter les instructions *B, C* et *E* comme précédemment, mais il doit également traiter le cas où *E* est omise. Cela peut être réalisé en exécutant le programme avec les conditions *a* et *d* vraies (exécution de B et de E), puis en exécutant le programme avec les conditions *a* et *d* fausses (exécution de C seule).

4.5.77 La couverture des tests des schémas descriptifs de matériel est un cas spécial et relève des schémas nationaux.

4.5.78 Les évaluateurs peuvent utiliser la *correspondance entre les tests et les fonctions dédiées à la sécurité et touchant à la sécurité dans la conception détaillée* ainsi que la *correspondance entre les tests et les mécanismes de sécurité tels qu'ils sont représentés dans le code source ou les schémas descriptifs des matériels* comme une aide pour vérifier la couverture.

4.5.79 Certains compilateurs disposent de fonctions pour surveiller les lignes de code source qui sont exécutées pendant les tests. Ces fonctions peuvent être utilisées par les développeurs pour produire des correspondances de tests. Les évaluateurs peuvent les utiliser pour vérifier la couverture des tests, pourvu qu'ils aient confiance dans la précision de ces fonctions.

4.5.80 Les évaluateurs sont tenus de *vérifier que tous les tests ont été repassés après la correction des erreurs*. Cela concerne les tests de non régression, c'est-à-dire les tests repassés après avoir corrigé les erreurs découvertes par les évaluateurs ou les développeurs.

4.5.81 Le principe sous-jacent repose ici sur le fait que les corrections apportées devraient être cohérentes avec la conception détaillée. Si la cible d'évaluation est modifiée après la détection d'une erreur, les composants modifiés devraient être testés à nouveau. De plus, certaines parties des tests du système devraient être répétées pour vérifier qu'aucune erreur secondaire n'a été introduite.

4.5.82 ***Les évaluateurs doivent passer en revue les déclarations du développeur concernant les tests de non régression dans le plan de test pour s'assurer que les tests sont repassés de façon adéquate. Les évaluateurs doivent assurer que la stratégie de tests de non régression est suivie.***

4.5.83 Les évaluateurs sont tenus de *réaliser des tests complémentaires pour rechercher des erreurs*. ***Les évaluateurs doivent, par conséquent, effectuer au moins un test supplémentaire de chaque fonction dédiée à la sécurité ; le test doit être différent des tests fournis par le commanditaire. Lorsque cela n'est pas approprié, un argumentaire doit être donné pour toute restriction au niveau des tests.*** Aux niveaux E1 et E2, les tests se feront par rapport à la cible de sécurité.

4.5.84 ***De plus, du niveau E3 au niveau E6, un test complémentaire de chaque fonction dédiée ou touchant à la sécurité doit être effectué ; le test doit être différent des tests fournis par le commanditaire. Lorsque ceci n'est pas approprié, un argumentaire doit être donné pour toute restriction au niveau des tests.*** Les tests réalisés se feront par rapport à la conception détaillée et au code source.

4.5.85 Les évaluateurs, en réalisant ces tests complémentaires, peuvent spécifier les tests, puis s'assurer du concours du commanditaire pour effectuer les tests. ***Dans ce cas, les évaluateurs doivent assister à l'exécution des tests.*** Sinon, les évaluateurs peuvent décider d'exécuter ces tests fonctionnels comme une partie des tests de pénétration (voir ci-dessous).

4.5.86 ***Les évaluateurs doivent également vérifier que les résultats effectifs des tests sont conformes aux résultats attendus.***

4.5.87 ***Si le commanditaire demande des informations pour la réévaluation dans le chapitre 7 du RTE, les évaluateurs doivent réunir les informations nécessaires au cours de cette activité.***

Vérifier l'environnement de développement

4.5.88 Les évaluateurs devraient examiner de manière informelle la documentation sur l'environnement de développement.

4.5.89 A partir du niveau E2, les évaluateurs sont tenus de *vérifier que les procédures documentées sont appliquées*. La méthode recommandée pour ce faire est d'effectuer une ou plusieurs visites sur le site du développement. Le but de ces visites est :

a) d'obtenir une meilleure compréhension du processus de développement en l'observant dans la pratique ;

b) de vérifier que les pratiques documentées sont appliquées dans la pratique.

4.5.90 La visite doit être convenue avec le développeur. Avant la visite, les évaluateurs devraient préparer une liste de contrôle des sujets dont ils souhaitent traiter. Cette liste peut être donnée au développeur pour lui permettre de préparer la visite.

4.5.91 Lors de cette visite, les évaluateurs devraient avoir un entretien avec le personnel de développement et auditer la gestion de configuration ainsi que les pratiques de sécurité.

4.5.92 Les évaluateurs sont tenus (à partir du niveau E4) d'*utiliser les outils des développeurs pour régénérer des parties sélectionnées de la TOE et comparer le résultat avec la version de la TOE soumise à l'évaluation*. Ceci constitue l'une des deux tâches autorisant l'échantillonnage.

4.5.93 ***Les évaluateurs doivent utiliser tous les processus de génération.*** Si le processus de génération est uniforme (tous les composants sont générés de la même façon), il suffit de régénérer un seul composant. ***Si chaque composant est généré différemment, les évaluateurs doivent régénérer tous les composants.*** Il est peu probable que les évaluateurs puissent générer des composants matériels. ***En ce qui concerne les composants matériels, les évaluateurs doivent assister à la fabrication de ces composants sur le site du développement.***

4.5.94 Les évaluateurs peuvent avoir besoin d'utiliser le système de développement pour effectuer cette tâche des ITSEC. Cela devrait être abordé dans le contrat passé avec le commanditaire.

4.5.95 Les outils de comparaison de fichiers peuvent être utilisés pour comparer le composant régénéré avec l'original. A noter que si le processus de génération produit un horodatage dans le composant, celui-ci ne sera pas conforme à l'original.

4.5.96 ***Si des informations pour la réévaluation sont exigées dans le RTE, les évaluateurs doivent identifier les outils de développement qui touchent à la sécurité.***

Vérifier la documentation d'exploitation

4.5.97 Cette vérification se fait par un examen informel et une revue. Les évaluateurs se familiarisent avec la documentation d'exploitation et s'assurent que l'information exacte est donnée et qu'elle suffit pour permettre d'utiliser et de configurer de manière sûre la cible d'évaluation.

Vérifier l'environnement d'exploitation

4.5.98 Cette vérification se fait par un examen informel. Les évaluateurs devraient se familiariser avec la documentation qui concerne la livraison, la configuration, le démarrage et l'exploitation et s'assurer que l'information exacte est donnée et qu'elle suffit pour permettre la maintenance et l'exploitation sûres de la cible d'évaluation. À partir du niveau E2, les évaluateurs auront besoin d'obtenir des informations de l'organisme de certification sur la *procédure... afin de garantir l'authenticité de la cible d'évaluation livrée*, exigée pour ces niveaux.

Exécuter les tests de pénétration

4.5.99 Le processus décrit ci-dessous, qui s'appuie sur [LINDE], peut être suivi pour sélectionner les tests de pénétration :

a) les évaluateurs listent toutes les erreurs, les incohérences et les vulnérabilités découvertes au cours de l'évaluation ;

b) les évaluateurs identifient dans cette liste les éléments qui peuvent conduire à des brèches dans la sécurité et dont la démonstration devrait pouvoir être faite dans la pratique par les tests de pénétration ;

c) les évaluateurs hiérarchisent les éléments retenus de manière à ce que ceux qui ont le plus de chance de pouvoir être testés soient effectués en premier et que ceux qui ont le moins de chance de pouvoir être testés soient effectués en dernier.

4.5.100 ***Afin que les tests puissent être répétés, les évaluateurs doivent rédiger un scénario de test, qui décrit la procédure pour effectuer chaque test de pénétration, et les résultats attendus du test.*** Les schémas nationaux peuvent comporter leurs propres exigences pour le test réalisé en dehors du CESTI (par exemple, sur les sites du développeur).

4.5.101 Les évaluateurs devraient informer le commanditaire de leurs besoins pour les tests de pénétration. Ceux-ci peuvent comprendre :

a) un accès adéquat à la cible d'évaluation ;

b) une assistance technique du développeur ;

c) un espace de travail, qui peut comprendre des lieux de stockage sûrs ;

d) l'utilisation de supports magnétiques.

4.5.102 Les tests de pénétration peuvent affecter ou endommager la cible d'évaluation. Les évaluateurs devraient débattre avec les commanditaires des mesures à prendre pour minimiser ces risques, telles que des sauvegardes.

4.5.103 Bien que les tests de pénétration devraient, pour la plupart, être effectués selon des scénarios définis, les tests au pied levé (c'est-à-dire les tests ne bénéficiant pas d'un scénario de test préparé à l'avance) sont autorisés. ***Ces tests doivent, cependant, être justifiés et enregistrés avec suffisamment de détails pour qu'ils puissent être répétés.***

4.5.104 Les tests de pénétration peuvent être facilités par l'utilisation d'outils de configuration et d'audit pour la sécurité. Ces outils examinent la configuration d'un système et recherchent des vulnérabilités ordinaires, telles que des fichiers en lecture pour tous et des mots de passe manquants.

Sélection et utilisation des outils d'évaluation

Introduction

4.5.105 ***Lorsqu'un outil automatisé est utilisé pour établir un verdict d'évaluation, le RTE doit consigner suffisamment d'informations sur l'outil et sur la façon dont il a été utilisé pour permettre de répéter ce verdict.***

4.5.106 ***Toute utilisation d'outils de cette manière doit être acceptable pour l'organisme de certification.*** Afin d'éviter les travaux non valables, il est conseillé aux CESTI d'obtenir l'accord de l'organisme de certification avant d'utiliser des outils.

4.5.107 Les organismes de certification peuvent, s'ils le souhaitent, conserver une liste des outils automatisés qui peuvent être utilisés pour effectuer certaines tâches de l'évaluateur des critères ITSEC.

Outils d'évaluation

4.5.108 Cette sous-section décrit brièvement les types d'outils qui pourraient être utiles aux évaluateurs.

4.5.109 *Les outils d'animation* : ils sont utilisés dans les phases amont d'un développement pour vérifier les représentations de haut niveau, telles que la cible de sécurité. Ces outils peuvent être exploités de la manière suivante :

a) convertir la représentation à animer en une spécification formelle exécutable ;

b) exécuter la spécification formelle afin de tester les propriétés de la représentation.

4.5.110 L'expérience pratique semble indiquer que la production de la spécification formelle est au moins aussi précieuse que son exécution.

4.5.111 *Les outils de génie logiciel :* lorsqu'un outil de génie logiciel a été utilisé pour produire une conception détaillée, les évaluateurs peuvent tenter d'utiliser l'outil pour effectuer une validation indépendante de la conception à l'aide des fonctions de validation que fournit l'outil. Elle peut être réalisée en utilisant l'outil pour analyser la conception et en utilisant ses fonctions de génération de rapports pour identifier les erreurs et les omissions, telles que :

a) les flux de données qui ne sont pas cohérents entre les diagrammes à différents niveaux de la hiérarchie de conception ;

b) les systèmes de stockage de données qui ont des flux de données en entrée mais pas en sortie (c'est-à-dire que les données sont produites, mais ne sont pas utilisées par un processus) ;

c) les objets (par exemple, les éléments de données, les flux de données ou les systèmes de stockage de données) qui sont définis, mais ne sont pas référencés par un processus ;

d) les références à des objets indéfinis.

4.5.112 *Les outils de vérification de la conception détaillée* peuvent être divisés en :

a) *outils de "conformité aux règles"* : ils vérifient que la syntaxe et la sémantique du code source correspondent à sa spécification. Ils proviennent souvent d'une évolution des outils de vérification de code source,

b) *outils de démonstration* : ils sont capables de réaliser la démonstration symbolique d'une conformité partielle ou totale :

- à un niveau syntaxique : complétude, cohérence, conformité,

- à un niveau sémantique : validité partielle ou totale,

c) *outils de suivi* : ils sont capables d'analyser et de rapporter sous une forme textuelle et graphique les graphes d'exécution d'un programme d'application, de générer le graphe d'appel des procédures et de fournir des références croisées. Cette catégorie comprend les analyseurs syntaxiques, les vérificateurs sémantiques, les analyseurs statiques, etc,

d) *outils de rétro-ingénierie* : ils sont capables de recréer et d'établir des liens entre les fonctions et les spécifications,

e) *outils d'analyse de canaux cachés* : la présence de canaux cachés peut être recherchée à l'aide d'une analyse des flux d'information. Cette vérification montrerait qu'il est impossible de faire circuler des informations entre les processus de façon non spécifiée.

4.5.113 *Les outils d'analyse du code source* peuvent être divisés en :

a) *analyseurs de l'utilisation des données* : ils recherchent dans le code source d'un programme l'utilisation incorrecte de données, telles que la lecture d'éléments de données avant qu'ils ne soient écrits ;

b) *analyseurs de flot de contrôle* : ils recherchent les erreurs de flot de contrôle, telles que les boucles sans sortie ou les codes inaccessibles ;

c) *analyseurs des flux d'information* : ils examinent les dépendances entre les éléments de données pour rechercher des dépendances indésirables ;

d) *analyseurs de concordance* : ils comparent la fonctionnalité du code source avec une spécification formelle et tâchent d'en prouver la concordance.

4.5.114 *Les outils d'analyse de code objet :* au niveau E6, le commanditaire est tenu de fournir aux évaluateurs des outils pour détecter les incohérences entre le code source et le code objet. Ces outils peuvent être utilisés pour examiner les incohérences soupçonnées.

4.5.115 *Les outils de génération* : à partir du niveau E3, des langages de programmation bien définis sont obligatoires. L'exemple 1(b) dans la partie 5 de l'ITSEM fournit un exemple qui illustre comment effectuer les tâches de l'évaluateur pertinentes. Au niveau E5, le code source de toutes les bibliothèques d'exécution doit être fourni. Par conséquent, les outils de compilation pour traiter ces informations sont utiles.

4.5.116 Au niveau E4, les évaluateurs utilisent les outils du développeur pour régénérer des parties sélectionnées de la cible d'évaluation et comparer les résultats avec la version de la cible d'évaluation soumise à l'évaluation. C'est dans ce sens que les compilateurs et autres outils de génération peuvent être utiles pour l'évaluation. C'est pourquoi il est nécessaire que les évaluateurs soient familiarisés avec les utilisations (et les abus possibles) de tels outils.

4.5.117 Si un compilateur devient une partie de confiance du système (par exemple, si les développeurs de logiciels malveillants sont désignés comme une menace dans la cible de sécurité), alors il sera soumis à une évaluation selon la procédure normale. Cela concerne, en particulier, les chevaux de Troie transitifs.

4.5.118 *Les outils de tests* : il existe des outils pour certains compilateurs qui peuvent enregistrer les lignes du code source qui ont été exécutées dans une séquence de tests. Ils peuvent constituer des éléments de preuve de la couverture des tests.

4.5.119 Les évaluateurs peuvent avoir besoin de développer du logiciel pour effectuer des tests de pénétration. Les évaluateurs peuvent également souhaiter avoir accès aux outils de tests propre au développeur (tels que les bancs d'essai et les outils de surveillance).

4.5.120 ***Toute utilisation d'outils de tests doit être documentée dans le RTE. Le logiciel de test utilisé par les évaluateurs doit être archivé.***

4.5.121 *Les outils d'analyse du matériel* : l'évaluation du matériel exige l'aide d'outils différents des outils adaptés à l'évaluation du logiciel. Les différences tournent autour de l'utilisation des outils de CAO et du fait qu'une analyse de code est inapplicable. Les outils de CAO peuvent être considérés comme des outils d'aide à la conception (comme les outils de génie logiciel) et tout ce qui a été dit ci-dessus concernant les outils de conception reste vrai pour les outils de CAO. A noter qu'il est peu probable qu'il soit possible de fournir des éléments de preuve d'une réalisation correcte suffisants sans utiliser les outils de CAO lors du développement, sauf pour des dispositifs extrêmement simples. Les outils de CAO peuvent fournir les services suivants :

a) bibliothèques de dispositifs ;

b) saisie de schémas (progiciels de tracé) ;

c) création de listes d'interconnexions ;

d) simulation ;

e) conception de circuits imprimés ;

f) test.

4.5.122 *Les outils d'audit et de configuration* : pour un certain nombre de systèmes d'exploitation largement répandus, il existe des outils d'audit et de configuration de la sécurité. De tels outils seront probablement utiles lors des tests de pénétration.

4.5.123 Un outil de configuration de la sécurité examine la façon dont un système d'exploitation a été configuré, en cherchant des vulnérabilités génériques connues, telles que les fichiers en lecture pour tous et les mots de passe faciles à deviner.

4.5.124 Un outil d'audit de la sécurité examine une **trace d'audit** et recherche des preuves de violation de la sécurité.

Résumé : Outils et techniques conseillés

4.5.125 La figure 4.5.1 fournit une analyse des techniques utiles aux évaluateurs. Ce tableau a été réalisé en considérant les activités individuelles de l'évaluateur.

4.5.126 De la même façon, la figure 4.5.2 fournit une analyse des outils utiles aux évaluateurs. D'autres outils peuvent être utilisés si cela améliore la fiabilité des résultats ou le coût de l'évaluation.

Figure 4.5.1 Techniques d'évaluation

Niveau d'éval ITSEC	Activités de l'évaluateur (les activités s'ajoutent d'un niveau à l'autre)	TECHNIQUES (les techniques s'ajoutent d'un niveau à l'autre)
E1	Vérifier la conception générale Vérifier la réalisation	examen informel ou analyse de concordance, tests fonctionnels tests de pénétration
E2	Vérifier la conception détaillée Vérifier la réalisation	examen informel ou analyse de concordance analyse de couverture de test tests de pénétration
E3	Vérifier la réalisation	analyse de couverture de test du code source tests de pénétration
E4	Vérifier la spécification des besoins Vérifier la conception générale Vérifier la conception détaillée	examen semi-formel ou analyse de concordance examen du modèle formel de politique de sécurité examen semi-formel ou analyse de concordance examen semi-formel ou analyse de concordance
E5	Vérifier la conception détaillée	examen semi-formel ou analyse de concordance examen du découpage en couche, de l'abstraction et du masquage des données de la conception
E6	Vérifier la conception générale	examen formel ou analyse de concordance
Tous	Vérifier l'environnement de développement	examen informel visites sur les sites de développement
Tous	Vérifier la documentation d'exploitation	examen informel
Tous	Vérifier l'environnement d'exploitation	examen informel
Tous	Vérifier l'analyse de pertinence	examen
Tous	Vérifier l'analyse de cohésion	examen, y compris la recherche de canaux cachés (le cas échéant)
Tous	Examiner la résistance des mécanismes	examen
Tous	Examiner les vulnérabilités de construction	examen analyse de vulnérabilité AMDE (le cas échéant)
Tous	Examiner la facilité d'emploi	examen
Tous	Examiner les vulnérabilités en exploitation	examen analyse de vulnérabilité

Figure 4.5.2 Outils d'évaluation

Niveau d'éval. ITSEC	Activités de l'évaluateur	OUTILS (les techniques s'accumulent d'un niveau sur l'autre)
E1	Vérifier la réalisation	outils et programmes de test (facultatif)
E2		
E3	Vérifier la réalisation	outils pour le contrôle de la couverture de test (facultatif)
E4	Vérifier la spécification des besoins Vérifier la conception générale Vérifier la conception détaillée Vérifier l'environnement de développement	outils de simulation (facultatif) outils de génie logiciel du développeur (facultatif) outils de génie logiciel du développeur (facultatif) outils de génération du développeur
E5	Vérifier la réalisation	outils d'analyse du code source (facultatif)
E6	Vérifier la conception générale Vérifier la réalisation	outils de vérification de démonstration (facultatif) outils permettant de découvrir des incohérences entre les codes source et exécutable (c.à.d. désassembleurs et outils d'aide à la mise au point)
E3-E6	Vérifier l'analyse de cohésion	outils d'analyse du code source et de manipulation de matrices (facultatif)

Chapitre 4.6 Réutilisation des résultats d'une évaluation

Introduction

4.6.1 Une évaluation est un processus complexe qui demande du temps et des ressources importantes. La charge dépensée et le prix à payer peuvent être considérables, selon le niveau d'évaluation visé et la complexité de la cible d'évaluation. Afin de limiter l'importance des travaux nécessaires, il est possible d'utiliser les résultats d'évaluations précédentes :

a) pour l'évaluation d'une cible d'évaluation qui comprend une ou plusieurs cibles d'évaluation déjà évaluées ;

b) pour la réévaluation d'une cible d'évaluation déjà certifiée après que la cible d'évaluation, sa cible de sécurité ou ses fournitures aient été modifiées.

4.6.2 Ce chapitre donne des avis aux évaluateurs pour la réutilisation des résultats d'une évaluation.

4.6.3 Le chapitre 4.3 traite les fournitures qui concernent les réutilisations et les réévaluations.

4.6.4 La partie 6, le chapitre 6.3 et l'annexe 6.D apportent des conseils au commanditaire/développeur en ce qui concerne les analyses d'impact après la modification d'une cible d'évaluation déjà certifiée.

Généralités

4.6.5 Les exemples suivants illustrent l'intérêt que peut présenter la réutilisation des résultats d'une évaluation :

a) les produits ou systèmes qui sont composés de plus d'un produit dont au moins un composant a déjà été évalué en tant que produit ;

b) les produits et les systèmes qui ont déjà été évalués et qui ont fait l'objet d'un changement qui rend nécessaire une réévaluation (par exemple, dans le cas d'une nouvelle édition d'un produit) ;

c) la composition de produits qui ont déjà été évalués à différents niveaux d'évaluation (profils d'assurance) ;

d) l'installation d'un système qui est constitué d'un produit déjà évalué ;

e) l'augmentation du niveau d'évaluation d'un produit déjà évalué ;

f) la modification d'une cible d'évaluation, de sa cible de sécurité, ou de l'une des fournitures (par exemple, une nouvelle édition d'un produit).

4.6.6 En général, il est plus ou moins nécessaire et utile de réutiliser des résultats d'une évaluation en fonction de :

a) l'utilisation de la cible d'évaluation déjà évaluée ;

b) la fonctionnalité de la cible d'évaluation déjà évaluée ;

c) du niveau d'évaluation atteint ;

d) de la cible de sécurité de la nouvelle cible d'évaluation dans laquelle sera incorporée la cible d'évaluation déjà évaluée.

4.6.7 Les conseils génériques donnés aux évaluateurs dans ce chapitre sont orientés vers les produits ou systèmes qui sont composés de plus d'un produit dont au moins une partie a déjà été évaluée comme un produit.

4.6.8 La réutilisation des cibles d'évaluation déjà évaluées dans un contexte différent de celui qui est spécifié dans la cible de sécurité pour la première évaluation est encore, dans une large mesure, du domaine de la recherche. Le sujet débattu ici est étroitement lié aux problèmes rencontrés dans le domaine de l'homologation de systèmes.

Conseils génériques pour l'évaluateur

4.6.9 Dans tous les cas où un doute subsiste sur les modalités de l'application des ITSEC et en l'absence de conseils dans l'ITSEM, l'organisme de certification devra être consulté. Cela devrait être le cas, par exemple, pour les cibles d'évaluation qui sont formées de composants évalués à différents niveaux d'évaluation.

4.6.10 Il n'est généralement pas possible de prévoir le niveau d'évaluation d'une composition étant donné les niveaux d'évaluation de ses composants. La composition peut atteindre un niveau d'évaluation inférieur au minimum des niveaux d'évaluation des composants, ou même un niveau supérieur au maximum des niveaux des composants, les fournitures exigées étant données. Cela est dû aux dépendances décrites au paragraphe 4.6.6. La résistance d'une combinaison peut également dépendre du type d'objectifs de sécurité comme la confidentialité, l'intégrité et la disponibilité.

4.6.11 L'assurance dans la composition ne peut être obtenue qu'après une évaluation, en particulier, après une analyse de l'efficacité réalisée à la fois par le commanditaire/développeur et l'évaluateur.

4.6.12 Différentes approches ont été proposées pour ce problème. Une des approches consiste à utiliser une *partition fonctionnelle* [TNI]. Une autre est fournie par des *ordres partiels sur des sous-ensembles de la Base Informatique de Confiance* [TDI]. Le principe utilisé dans les systèmes à machines virtuelles est le strict cloisonnement mis en application par un noyau à échange de messages. Le modèle de composition présenté dans l'annexe 6.F de la partie 6 peut également guider les évaluateurs dans l'exécution de leur travail de réévaluation.

4.6.13 Les paragraphes suivants présentent les règles fondamentales qui s'appliquent aux cibles d'évaluation composées au minimum de deux composants dont au moins un a déjà été évalué au même niveau d'évaluation que la cible d'évaluation composée. Si plus d'un composant a déjà été évalué, il est supposé que tous les composants ont été évalués au même niveau d'évaluation.

4.6.14 Comme pour toute autre cible d'évaluation, il doit exister une cible de sécurité pour la composition. Il doit être possible d'établir une correspondance entre les cibles de sécurité des composants et la cible de sécurité de la composition. Une vérification de cela doit faire partie de l'analyse de la pertinence.

4.6.15 L'évaluation de la cible d'évaluation composée selon les critères d'efficacité doit être effectuée quelles que soient les circonstances.

4.6.16 L'analyse de la pertinence doit établir si les caractéristiques de sécurité des composants individuels constituent les caractéristiques de sécurité déclarées de la cible d'évaluation composée.

4.6.17 L'analyse de la cohésion pour la cible d'évaluation composée doit être faite tout comme celle effectuée pour l'évaluation d'une cible d'évaluation non composée.

4.6.18 Les évaluateurs doivent vérifier que l'interface fournie par un composant n'est utilisée et ne peut être utilisée que dans la composition de sorte que les caractéristiques de sécurité de la cible d'évaluation composée ne soient pas compromises.

4.6.19 L'analyse des vulnérabilités de construction doit être fondée sur les relations d'"utilisation" des composants individuels. Les détails internes du composant "utilisé" ne devraient pas compromettre les hypothèses émises pour le composant "utilisateur". Il faut également estimer si une vulnérabilité potentielle d'un composant est exploitable dans le contexte de la composition. La liste des vulnérabilités identifiées lors de l'évaluation d'un seul composant peut contenir des vulnérabilités qui ne sont pas significatives lorsque le composant est utilisé dans une composition.

4.6.20 L'analyse de la facilité d'emploi pour la cible d'évaluation composée doit être réalisée de la même façon que celle effectuée lors de l'évaluation d'une cible d'évaluation non composée.

4.6.21 Pour un composant déjà évalué et utilisé dans une composition, les critères de conformité pour le processus de développement n'ont pas besoin d'être à nouveau évalués. Les évaluateurs peuvent supposer que les verdicts de conformité restent vrais. Cela ne s'applique pas aux tests concernant l'efficacité dans le nouveau contexte.

4.6.22 L'évaluation de la conformité de la cible d'évaluation vue dans son ensemble est toujours exigée, même si la cible d'évaluation est entièrement constituée de composants déjà évalués. La cible de sécurité, la conception générale, l'environnement de développement et les tests de la cible d'évaluation dans son ensemble devraient, par conséquent, être évalués. L'évaluation complète de la conformité selon les critères ITSEC et l'ITSEM est exigée pour les composants de la cible d'évaluation qui n'ont pas déjà subi une évaluation.

4.6.23 Si la composition concerne la documentation utilisateur et d'administration, alors les critères des ITSEC sur la documentation d'exploitation devront être appliqués.

4.6.24 Les critères des ITSEC qui portent sur l'environnement de développement, aspect 1 - gestion de la configuration, et ceux qui concernent l'environnement d'exploitation doivent être appliqués comme pour l'évaluation d'une cible d'évaluation non composée. Il n'y a rien à faire pour ces aspects en ce qui concerne le composant déjà évalué.

Chapitre 4.7 Résultats de l'évaluation

Introduction

Objectifs

4.7.1 Ce chapitre fournit une description détaillée des résultats de l'évaluation exigés, à savoir le RTE et les rapports d'anomalie.

Champ d'application

4.7.2 Le chapitre 4.4 décrit la rédaction de rapports d'évaluation comme une partie du processus d'évaluation. Ce chapitre traite principalement du RTE qui est rédigé par les évaluateurs à l'attention du commanditaire de l'évaluation et de l'organisme de certification.

4.7.3 Les schémas nationaux exigeront des rapports d'évaluation supplémentaires, tels que des rapports sur les méthodes d'évaluation, des rapports d'anomalie, ou des rapports sur les travaux à l'échelle individuelle. Ce sont des questions concernant les schémas nationaux et elles ne sont traitées dans ce chapitre que lorsqu'elles affectent le contenu du RTE.

Résumé

4.7.4 Il est supposé, tout au long de ce chapitre, que le RTE est un seul document, qui est le résultat de l'activité *Rédaction des rapports* décrite au chapitre 4.4. Les schémas nationaux peuvent ne tenir aucun compte de cette hypothèse et mettre en place des dispositions différentes.

4.7.5 Par exemple, il est affirmé plus loin dans ce chapitre qu'une partie du RTE décrit la cible de sécurité de la cible d'évaluation. Un schéma national peut prendre des dispositions pour que le RTE incorpore la cible de sécurité ou pour qu'il fasse référence à la cible de sécurité (c'est-à-dire en publiant le RTE conjointement avec la cible de sécurité).

4.7.6 L'incorporation d'un PTE pour remplacer le chapitre qui décrit les travaux d'évaluation est un autre exemple. Le PTE devrait alors au moins contenir les points qui sont résumés au paragraphe 4.7.42.

4.7.7 Un RTE vise les objectifs suivants :

a) décrire les travaux réellement effectués lors de l'évaluation ;

b) présenter les résultats obtenus et les conclusions tirées de ces travaux.

4.7.8 L'audience visée d'un RTE est :

a) l'organisme de certification ;

b) le commanditaire de l'évaluation ;

c) les évaluateurs qui effectuent une réévaluation..

4.7.9 Lorsque le commanditaire et le développeur ne sont pas confondus, les schémas nationaux devraient également prendre des dispositions pour communiquer tout ou partie du RTE à l'attention des développeurs qui étudient la possibilité de réutiliser une cible d'évaluation comme une partie d'une autre cible d'évaluation. Des dispositions devraient être prises concernant la publication du RTE dans un autre pays. La façon de procéder relève des schémas nationaux.

4.7.10 L'organisme de certification est responsable de l'acceptation du RTE.

4.7.11 Ce chapitre identifie les exigences minimales qui concernent le *contenu et l'organisation du RTE* (via les intitulés des chapitres et sections) et traite du contenu de chaque chapitre et de chaque section tour à tour.

Contenu et organisation du Rapport Technique d'Évaluation

Avant-propos

4.7.12 Les schémas nationaux ont à définir les règles obligatoires de marquage et de gestion des RTE et décrivent la forme de l'avant-propos dans un RTE. Par exemple, pour les systèmes gouvernementaux, le RTE peut être classifié ; pour les systèmes et produits commerciaux, le RTE peut avoir à porter des marques de protection.

4.7.13 Pourraient figurer dans l'avant-propos :

a) les limites de responsabilité ;

b) les logotypes du schéma ;

c) les clauses de copyright.

Corps du document

4.7.14 La figure 4.7.1 propose une organisation pour le RTE. Cette structure sera vraisemblablement affinée au fur et à mesure que l'expérience de l'évaluation augmentera.

4.7.15 Le contenu de chaque chapitre/section identifié est décrit ci-après. Les schémas nationaux peuvent choisir de proposer plusieurs organisations de RTE. Cependant, le contenu technique fourni doit couvrir les éléments décrits ci-dessous.

4.7.16 ***A noter qu'un RTE doit fournir la justification de tous les verdicts prononcés par les évaluateurs. Aucune référence à un élément inaccessible ne doit être faite.***

Chapitre 1 du RTE - Introduction

Contexte

4.7.17 ***Cette section comporte une présentation du contexte de l'évaluation. Elle doit comprendre :***

a) ***l'identifiant de l'évaluation attribué par l'organisme de certification ;***

b) ***le nom et la version de la cible d'évaluation évaluée ;***

c) ***l'identité du développeur (y compris des sous-traitants si nécessaire) ;***

d) ***l'identité du commanditaire ;***

e) ***la durée totale de l'évaluation ;***

f) ***l'identité du CESTI.***

Objectifs

4.7.18 ***Cette section doit présenter les objectifs du RTE (comme indiqué ci-dessus).***

4.7.19 Les objectifs, à un niveau plus détaillé, sont :

a) de présenter les éléments de preuve qui étayent les verdicts et les conclusions de l'évaluation ;

b) d'étayer la réévaluation de la cible d'évaluation, si cela est demandé par le commanditaire.

4.7.20 L'alinéa b) ci-dessus est particulièrement important si les évaluations doivent avoir un bon bilan économique. Les informations à fournir dans le RTE sont plus nombreuses que si seul le cas de l'alinéa a) était considéré. Les évaluateurs devraient se rappeler ce point tout au long de l'évaluation et plus particulièrement lorsqu'ils rédigent les RTE.

Champ d'application

4.7.21 ***Cette section doit préciser que le RTE couvre toute l'évaluation. Dans le cas contraire, une justification doit être fournie.***

Organisation

4.7.22 ***Cette section doit présenter l'organisation du RTE.*** Les écarts par rapport à l'organisation du RTE suggérée dans ce chapitre seront organisés par les schémas nationaux.

Chapitre 2 du RTE - Résumé général

4.7.23 Ce chapitre est à la base de toute information qui concerne les résultats de l'évaluation qui est publiée par l'organisme de certification.

4.7.24 Lorsque les schémas nationaux produisent des listes de cibles d'évaluation certifiées, ce chapitre constitue la base des informations se trouvant dans ces listes.

4.7.25 ***Le résumé général ne doit pas, par conséquent, contenir des informations qui sont susceptibles d'être sensibles sur le plan national ou commercial de quelque façon que ce soit (le commanditaire et l'organisme de certification le confirmeront lors de l'acceptation du RTE).***

4.7.26 ***Ce chapitre doit contenir :***

a) ***l'identité du CESTI ;***

b) ***le niveau d'évaluation réellement atteint ;***

c) ***l'identifiant de la cible d'évaluation ainsi que son numéro de version/numéro d'édition ;***

d) ***un résumé des principales conclusions de l'évaluation ;***

e) ***l'identité du commanditaire ;***

f) ***une brève description de la cible d'évaluation ;***

g) ***une brève description des caractéristiques de sécurité de la cible d'évaluation.***

Chapitre 3 du RTE - Description de la cible d'évaluation

Fonctionnalité de la cible d'évaluation

4.7.27 ***Cette section doit contenir un résumé du rôle opérationnel de la cible d'évaluation ainsi que les fonctions qu'elle assure et pour lesquelles elle a été conçue. Ce résumé comprend :***

a) ***le type de données à traiter (avec des niveaux de sensibilité si nécessaire) ;***

b) ***les différents types d'utilisateurs (en rapport avec ce qui est énoncé ci-dessus).***

Historique du développement

4.7.28 ***Cette section doit présenter (pour les évaluations simultanées, et si possible, pour les évaluations consécutives) les phases de développement de la production de la cible d'évaluation.***

4.7.29 ***Tous les cadres méthodologiques, les techniques, les outils et les normes de développement liés à la production de la cible d'évaluation, et qui ne sont pas traités dans le chapitre des résultats, doivent être brièvement évoqués.***

4.7.30 ***Les fournitures de l'évaluation de la cible d'évaluation doivent être mises en évidence (dont les détails, tels que l'état de publication, les dates, les numéros de référence et les auteurs seront subordonnés à l'annexe A du RTE).***

Conception générale de la cible d'évaluation

4.7.31 ***Cette section doit résumer la conception de plus haut niveau de la cible d'évaluation. Elle doit démontrer le degré de séparation entre les composants dédiés à la sécurité et les autres composants. Elle doit également souligner la répartition des fonctions dédiées à la sécurité de la cible d'évaluation entre les matériels, les microprogrammes et les logiciels (et éventuellement les procédures manuelles) à travers la conception générale de la cible d'évaluation.***

4.7.32 Tous les numéros de version des composants sont répertoriés dans l'annexe C du RTE.

Description des matériels

4.7.33 ***La description des matériels doit donner des détails appropriés sur tous les composants pertinents pour l'évaluation au niveau de la conception générale.***

Description des microprogrammes

4.7.34 ***La description des microprogrammes doit donner des détails appropriés sur tous les composants pertinents pour l'évaluation.***

Description des logiciels

4.7.35 ***La description des logiciels doit donner des détails appropriés sur toutes les parties du logiciel de la cible d'évaluation pertinents pour l'évaluation. La description doit lier les composants logiciels aux composants matériels et aux composants microprogrammés.***

Chapitre 4 du RTE - Caractéristiques de sécurité de la cible d'évaluation

4.7.36 Il est souligné qu'une compréhension du contenu de la cible de sécurité est essentielle à la compréhension du RTE. De plus, il est nécessaire d'avoir accès à la cible de sécurité et au RTE pour qu'une réévaluation soit efficace. ***Ce chapitre doit soit se référer à la cible de sécurité, soit reformuler la cible de sécurité dans son intégralité.***

4.7.37 Le contenu de ce chapitre est résumé ci-dessous. Les ITSEC contiennent de plus amples informations (chapitre 2 et annexe A).

a) politique de sécurité du système / argumentaire du produit ;

b) spécification des fonctions dédiées à la sécurité ;

c) spécification des mécanismes de sécurité ;

d) cotation annoncée de la résistance minimale des mécanismes ;

e) niveau d'évaluation visé.

Chapitre 5 du RTE - Évaluation

4.7.38 Le chapitre 4.4 traite du processus à utiliser pour l'évaluation et pour la production effective du PTE. Le chapitre 5 du RTE décrit en détail les travaux d'évaluation réalisés en faisant notamment état de tout problème rencontré (technique ou de conduite). Le chapitre a pour objet de faciliter le processus d'analyse au sein des organismes de certification afin que le processus d'évaluation dans son ensemble puisse être raffiné tant sur le plan technique que sur le plan de la conduite (et par conséquent, qu'il puisse être plus efficace et moins coûteux).

Historique de l'évaluation

4.7.39 Cette section est conçue de la même manière que la section de l'historique du développement du chapitre 3 énoncée ci-dessus. ***Elle doit présenter le processus d'évaluation utilisé et les étapes clefs qui :***

a) ***furent prévus au début de l'évaluation de la cible d'évaluation (par exemple, pour la production du PTE, du RTE etc.) ;***

b) ***ont réellement été atteints au cours de l'évaluation.***

4.7.40 Les étapes clefs peuvent comprendre :

a) toute réunion de lancement de l'évaluation ;

b) la livraison de la cible de sécurité ;

c) le moment où les tests de pénétration sont effectués ;

d) toute visite au(x) site(s) d'exploitation ou de développement de la cible d'évaluation ;

e) l'achèvement du travail technique.

4.7.41 ***Toutes les méthodes d'évaluation, techniques, outils et normes utilisés doivent être brièvement exposés.***

Procédure d'évaluation

4.7.42 ***Un résumé du PTE doit être fourni dans cette section. Ce résumé doit inclure :***

a) ***les*** *tâches de l'évaluateur* ***couvertes par le programme de travail et justifiées selon les ITSEC ;***

b) ***les*** *lots de travaux* ***effectués (en renvoyant au chapitre 4.5 de l'ITSEM pour démontrer l'utilisation des procédures acceptables et à l'annexe D du RTE pour les détails). Toute différence entre les travaux proposés dans le PTE et ceux effectués dans la pratique doit être soulignée et accompagnée d'un argumentaire permettant d'expliquer l'existence de ces divergences ;***

c) ***un résumé de la façon dont les fournitures de l'évaluation (répertoriées dans l'annexe A du RTE) ont correspondu aux*** *phases de construction* ***utilisées dans les critères ITSEC. Il doit inclure toutes les différences entre les phases de construction initialement envisagées et celles, qui se sont réellement déroulées ou qui ont été utilisées.***

Limites de l'évaluation

4.7.43 ***Cette section doit identifier avec précision les composants de la cible d'évaluation évaluée et toutes les hypothèses faites à propos des composants qui n'ont pas été examinés.***

Contraintes et hypothèses

4.7.44 ***Cette section doit souligner toute contrainte de l'évaluation et toute hypothèse faite au cours de l'évaluation.***

Chapitre 6 du RTE - Résumé des résultats de l'évaluation

4.7.45 ***Ce chapitre doit fournir des résumés des résultats de l'évaluation en termes des tâches de l'évaluateur identifiées par les ITSEC.*** La structure du chapitre, par conséquent, reflète dans les grandes lignes la structure des chapitres traitant de l'efficacité et de la conformité dans les ITSEC.

4.7.46 ***L'intitulé de chaque sous-section doit être le nom de la tâche de l'évaluateur correspondante pour chaque phase ou aspect.***

4.7.47 ***Chaque sous-section doit faire référence aux rapports issus des lots considérés. Ces rapports figurent dans ce chapitre ou forment l'annexe D du RTE.***

4.7.48 Les six premières sections sont simplement énumérées ci-dessous. Les paragraphes ultérieurs fournissent des explications sur les quatre dernières sections (tests de pénétration, vulnérabilités exploitables découvertes, observations concernant les vulnérabilités non exploitables et les erreurs découvertes).

a) Critères d'efficacité - Construction

- Aspect 1 - Pertinence de la fonctionnalité
- Aspect 2 - Cohésion de la fonctionnalité
- Aspect 3 - Résistance des mécanismes
- Aspect 4 - Estimation de la vulnérabilité de la construction

b) Critères d'efficacité - Exploitation

- Aspect 1 - Facilité d'emploi
- Aspect 2 - Estimation de la vulnérabilité en exploitation

c) Construction - Le processus de développement

- Phase 1 - Spécification des besoins
- Phase 2 - Conception générale
- Phase 3 - Conception détaillée
- Phase 4 - Réalisation

d) Construction - L'environnement de développement

- Aspect 1 - Gestion de configuration
- Aspect 2 - Langages de programmation et compilateurs
- Aspect 3 - Sécurité des développeurs

e) Exploitation - La documentation d'exploitation

- Aspect 1 - Documentation utilisateur
- Aspect 2 - Documentation d'administration

f) Exploitation - L'environnement d'exploitation

- Aspect 1 - Livraison et configuration
- Aspect 2 - Démarrage et exploitation

Tests de pénétration

4.7.49 Comme dans le chapitre 4.5, les résultats des tests de pénétration ont été traités séparément car les tests de pénétration sont généralement exécutés pour plus de commodité comme une partie d'un lot de travaux.

4.7.50 ***Toutes les options de configuration utilisées au cours des tests de pénétration doivent être enregistrées.***

4.7.51 ***Les résultats des tests de pénétration doivent renvoyer :***

a) ***au lot qui a été à l'origine de leur formulation ;***

b) ***à la tâche de l'évaluateur décrite comme obligatoire par les critères ITSEC.***

Vulnérabilités exploitables découvertes

4.7.52 ***Cette section doit décrire les vulnérabilités exploitables découvertes au cours de l'évaluation en identifiant :***

a) ***la fonction dédiée à la sécurité dans laquelle la vulnérabilité a été découverte ;***

b) ***une description de la vulnérabilité ;***

c) ***la tâche de l'évaluateur au cours de laquelle la vulnérabilité a été découverte ;***

d) ***le lot au cours duquel la vulnérabilité a été découverte ;***

e) ***la personne qui a découvert la vulnérabilité (évaluateur ou développeur) ;***

f) ***la date à laquelle la vulnérabilité a été découverte ;***

g) ***si la vulnérabilité a été corrigée (et à quelle date) ou non ;***

h) ***la source de la vulnérabilité (si possible).***

Remarques concernant les vulnérabilités non exploitables

4.7.53 ***Cette section doit rapporter les vulnérabilités non exploitables découvertes au cours de l'évaluation (en soulignant celles qui demeurent dans la cible d'évaluation opérationnelle).***

Erreurs découvertes

4.7.54 ***Cette section doit résumer l'impact des erreurs découvertes au cours du développement tel que perçu par les évaluateurs. Tout résultat ou conclusion concrets, fondés sur les erreurs découvertes, concernant la capacité de la cible d'évaluation à satisfaire le niveau d'évaluation visé doit être pleinement justifié.***

Chapitre 7 du RTE - Conseils pour la réévaluation et l'analyse d'impact

4.7.55 Ce chapitre est facultatif. Il peut être omis si le commanditaire a précisé qu'il n'exigeait pas d'informations pour la réévaluation ou l'analyse d'impact.

4.7.56 ***S'il existe, ce chapitre du RTE doit consigner (en identifiant la phase ou l'aspect de construction, ou l'aspect d'exploitation, avec les références aux fournitures de l'évaluation) :***

a) ***la classification de toutes les parties de la cible d'évaluation, à chaque phase de construction examinée, selon trois catégories : dédié à la sécurité, touchant à la sécurité et ne touchant pas à la sécurité (définies dans la partie 3 de l'ITSEM) ;***

b) ***l'identification des outils de développement de la cible d'évaluation qui touchent à la sécurité (définis dans la partie 3 de l'ITSEM) ;***

c) ***tout cas dans lequel les contraintes ou les hypothèses de l'évaluation pourraient avoir un impact sur la réévaluation ou la réutilisation ;***

d) ***toutes les leçons concernant les techniques ou les outils d'évaluation qui seraient utiles pour une réévaluation (les schémas nationaux peuvent décider de produire un document indépendant pour les consigner) ;***

e) ***tous les détails concernant l'archivage nécessaires au redémarrage de l'évaluation (les schémas nationaux peuvent décider de produire un document indépendant pour les consigner) ;***

f) ***toutes les compétences spécifiques qu'il est recommandé aux "réévaluateurs" d'avoir avant la réévaluation (les schémas nationaux peuvent décider de produire un document indépendant pour les consigner) ;***

g) ***la compréhension des évaluateurs des différentes façons de configurer la cible d'évaluation de sorte que cette dernière devienne non sûre.***

Chapitre 8 du RTE - Conclusions et recommandations

4.7.57 ***Les conclusions et les recommandations de l'évaluation doivent être décrites dans ce chapitre. La conclusion principale permet de savoir si la cible d'évaluation a satisfait à sa cible de sécurité et ne contient pas de vulnérabilité exploitable.***

4.7.58 Les recommandations sont normalement adressées à l'organisme de certification. Il doit être précisé que ces recommandations portent sur les parties de la cible d'évaluation qui s'inscrivent dans les limites de l'évaluation, et qu'il peut y avoir d'autres facteurs, que les évaluateurs ignorent, qui peuvent également influencer le contenu du certificat/rapport de certification de la cible d'évaluation.

4.7.59 Les recommandations peuvent comporter des suggestions à l'attention d'autres organisations, telles que le commanditaire ou le développeur, qui seront transmises par l'organisme de certification. Ces recommandations peuvent rappeler que les résultats de l'évaluation ne sont valides que pour une version particulière de la cible d'évaluation lorsqu'elle est configurée d'une certaine manière, et que l'organisme de certification doit être informé de toutes les modifications apportées à la cible d'évaluation comme il est indiqué dans l'annexe 6.D de la partie 6.

Annexe A du RTE - Liste des fournitures de l'évaluation

4.7.60 ***Cette annexe doit identifier, avec les numéros de version et les dates de réception, toutes les fournitures de l'évaluation (en général, la version la plus récente d'une fourniture est suffisante à moins que les résultats ne soient obtenus à partir de versions antérieures) ou faire une référence externe à la liste des fournitures.***

4.7.61 ***Toute différence entre les fournitures livrées et celles identifiées dans l'annexe 6.A de la partie 6 doit être soulignée et justifiée.***

Annexe B du RTE - Liste des acronymes/Glossaire terminologique

4.7.62 ***Cette annexe doit expliquer tous les acronymes ou abréviations utilisés dans le RTE. Elle doit également définir tous les termes utilisés qui n'apparaissent pas dans les glossaires de l'ITSEM ou des critères ITSEC.***

Annexe C du RTE - Configuration évaluée

4.7.63 ***Les configurations de la cible d'évaluation examinées lors de l'évaluation (en particulier, les configurations utilisées lors des tests de pénétration, de l'estimation de la facilité d'emploi et des travaux se rapportant à la cible d'évaluation opérationnelle) doivent être clairement identifiées.***

4.7.64 ***Toutes les hypothèses faites ou les configurations non prises en considération doivent être soulignées.***

Description des matériels

4.7.65 ***La description des matériels doit donner des informations sur la configuration de tous les composants au niveau de la conception générale qui sont pertinents pour l'évaluation (et par conséquent, aux fonctions dédiées à la sécurité).***

Description des microprogrammes

4.7.66 ***La description des microprogrammes doit donner des informations sur la configuration de tous les composants (comme décrits ci-dessus) qui sont pertinents pour l'évaluation (et par conséquent, aux fonctions dédiées à la sécurité et éventuellement aux fonctions touchant à la sécurité).***

Description des logiciels

4.7.67 ***La description des logiciels doit donner des informations sur la configuration des parties du logiciel de la cible d'évaluation qui sont pertinents pour l'évaluation (et par conséquent, aux fonctions dédiées à la sécurité et aux fonctions touchant à la sécurité).***

Annexe D du RTE - Rapports issus des lots

4.7.68 Cette annexe n'a pas besoin d'être produite si tous les rapports issus des lots sont contenus dans le chapitre 6 du RTE.

4.7.69 ***Si elle existe, cette annexe doit comprendre l'enregistrement de tous les travaux effectués (y compris l'échantillonnage des résultats de tests réalisé, les techniques et les outils utilisés) nécessaire pour justifier les verdicts prononcés lors de l'exécution des tâches de l'évaluateur.***

Annexe E du RTE - Rapports d'anomalie

4.7.70 Les schémas nationaux seront à l'origine des procédures pour consigner les problèmes. ***Tous les rapports d'anomalie émis doivent être intégrés dans cette annexe.*** Les rapports d'anomalie peuvent être délivrés avant la fin de l'évaluation. ***Les rapports d'anomalie doivent, au moins, contenir les éléments suivants :***

a) ***l'identifiant d'évaluation attribué par l'organisme de certification ;***

b) ***le nom et la version de la cible d'évaluation évaluée ;***

c) ***l'activité au cours de laquelle le problème a été rencontrée ;***

d) ***la description du problème.***

Figure 4.7.1 Organisation du RTE (1 de 2)

Chapitre 1 du RTE - Introduction

- Contexte
- Objectifs
- Champ d'application
- Organisation

Chapitre 2 du RTE - Résumé général

Chapitre 3 du RTE - Description de la cible d'évaluation

- Fonctionnalité de la cible d'évaluation
- Historique du développement
- Conception générale de la cible d'évaluation
  - Description des matériels
  - Descriptions des microprogrammes
  - Description des logiciels

Chapitre 4 du RTE - Caractéristiques de sécurité de la cible d'évaluation

- Politique de sécurité du système / argumentaire du produit
- Spécification des fonctions dédiées à la sécurité
- Spécification des mécanismes de sécurité
- Cotation annoncée de la résistance minimale des mécanismes
- Niveau d'évaluation visé

Chapitre 5 du RTE - Évaluation

- Historique de l'évaluation
- Procédure d'évaluation
- Limites de l'évaluation
- Contraintes et hypothèses

Figure 4.7.1 Organisation du RTE (2 de 2)

Chapitre 6 du RTE - Sommaire des résultats de l'évaluation

Critères d'éfficacité - Construction
- Aspect 1 - Pertinence de la fonctionnalité
- Aspect 2 - Cohésion de la fonctionnalité
- Aspect 3 - Résistance des mécanismes
- Aspect 4 - Estimation de la vulnérabilité de la construction

Critères d'efficacité - Exploitation
- Aspect 1 - Facilité d'emploi
- Aspect 2 - Estimation de la vulnérabilité en exploitation

Construction - Le processus de développement
- Phase 1 - Spécification des besoins
- Phase 2 - Conception générale
- Phase 3 - Conception détaillée
- Phase 4 - Réalisation

Construction - L'environnement de développement
- Aspect 1 - Gestion de configuration
- Aspect 2 - Langages de programmation et compilateurs
- Aspect 3 - Sécurité des développeurs

Exploitation - La documentation d'exploitation
- Aspect 1 - Documentation utilisateur
- Aspect 2 - Documentation d'administration

Exploitation - L'environnement d'exploitation
- Aspect 1 - Livraison et configuration
- Aspect 2 - Démarrage et exploitation

Tests de pénétration

Vulnérabilités exploitables découvertes

Remarques concernant les vulnérabilités non exploitables

Erreurs découvertes

Chapitre 7 du RTE - Conseils pour la réévaluation et l'analyse d'impact

Chapitre 8 du RTE - Conclusions et recommandations

Annexe A du RTE - Liste des fournitures de l'évaluation

Annexe B du RTE - Liste des acronymes/Glossaire terminologique

Annexe C du RTE - Configuration évaluée

Annexe D du RTE - Rapports issus des lots

Annexe E du RTE - Rapports d'anomalie

Partie 5 Exemples d’application des ITSEC

Table des matières

Figures

Chapitre 5.1 Introduction

Objectifs de cette partie

5.1.1 L'objectif est de démontrer, par des exemples, comment l'approche décrite dans l'ITSEM associée aux critères ITSEC peut être appliquée à l'évaluation de systèmes et de produits.

5.1.2 Rien dans cette partie n'est obligatoire. Elle a pour seul objet d'illustrer l'application des critères ITSEC et de l'ITSEM, et non pas de les développer.

5.1.3 Le but final est de fournir des exemples complets sur :

a) les évaluations simultanées ;

b) les évaluations consécutives ;

c) le logiciel ;

d) le matériel ;

e) les produits ;

f) les systèmes ;

g) la **réévaluation** ;

h) la **réutilisation** des résultats d'évaluation.

5.1.4 Les alinéas (d), (g) et (h) ci-dessus ne sont pas traités dans cette version de l'ITSEM, mais seront abordés dans les versions futures.

5.1.5 Les exemples 1 à 6 sont fondés sur l'expérience d'évaluations européennes antérieures aux critères ITSEC. Leurs origines sont des évaluations réelles, mais elles ont été nettoyées et reformulées dans les termes des critères ITSEC.

5.1.6 L'exemple 7 est théorique. Il est spéculatif par nature.

5.1.7 L'exemple 8 traite de la sécurité du développeur.

Correspondance entre la présente partie et les critères ITSEC

5.1.8 Les exemples traitent de :

a) l'examen de l'environnement de développement (pour E2 et E4) ;

b) l'examen de la conformité de la spécification des besoins (pour E4) ;

c) l'examen de la conformité de la conception générale (pour E4) ;

d) l'examen de la conformité de la conception détaillée (pour E2) ;

e) l'examen de la conformité de la réalisation (pour E2) ;

f) l'examen de la conformité de l'exploitation (principalement pour E2, mais avec des exemples à tous les niveaux qui traitent du concept *présenter, décrire* et *expliquer* dans le contexte d'un guide utilisateur) ;

g) l'estimation de l'efficacité (pour E3) ;

h) l'*examen de la sécurité des développeurs* (pour E2 et E4).

5.1.9 Les figures 5.1.1, 5.1.2 et 5.1.3 structurent les tâches de l'évaluateur sous la forme de tables. Les critères s'élaborent en tâches pour l'estimation de la conformité (figures 5.1.1 et 5.1.2) et en tâches pour l'estimation de l'efficacité (figure 5.1.3).

5.1.10 Les éléments des tables sont des références aux paragraphes de [ITSEC].

5.1.11 La convention suivante a été adoptée dans les lignes des tables. Un signe plus (`+') indique que des tâches d'évaluation supplémentaires ou que des **fournitures** supplémentaires sont exigées en plus de celles qui sont énoncées au niveau d'évaluation précédent. En d'autres termes, si une cellule ne comporte pas de signe plus, le paragraphe auquel il est fait référence est identique à celui qui est identifié par sa cellule de gauche.

5.1.12 Pour l'efficacité, les critères ne sont pas présentés séparément pour chaque niveau d'évaluation des critères ITSEC. L'estimation de l'efficacité est, cependant, effectuée avec une rigueur croissante en fonction du niveau d'évaluation visé, et ce essentiellement parce que le degré de compréhension acquis par l'évaluateur augmente avec le niveau d'évaluation.

5.1.13 Le corps principal de cette partie présente huit exemples. La couverture de chaque exemple est indiquée dans les figures 5.1.1, 5.1.2 et 5.1.3.

5.1.14 L'intitulé des exemples identifie l'activité d'évaluation ainsi que le niveau d'évaluation visé.

5.1.15 Dans cette partie, le terme ***rapport d'anomalie*** désigne l'enregistrement formel d'une **erreur** par les évaluateurs.

	E1	E2	E3	E4	E5	E6
Tâches "Spécification de Besoins"	E1.4	E2.4	E3.4	(2) E4.4+	E5.4	E6.4
Tâches "Conception Générale"	E1.7	E2.7+	E3.7	(3) E4.7	E5.7+	E6.7+
Tâches "Conception Détaillée"		(4) E2.10+	E3.10	E4.10	E5.10	E6.10
Tâches "Réalisation"	E1.13	(5) E2.13+	E3.13+	E4.13	E5.13	E6.13+

+ indique une rigueur accrue dans la tâche

indique que les tâches sont traitées dans les exemples

(n) **indique que les tâches sont traitées dans l'exemple n**

Figure 5.1.1 Tâches de l'évaluateur pour la conformité selon les critères ITSEC (i)

	E1	E2	E3	E4	E5	E6
Tâches "Gestion de Configuration"	E1.17	(1a) E2.17+	E3.17	E4.17+	E5.17+	E6.17
Tâches "Langages de Programmation et Compilateurs"			E3.20+	(1b) E4.20	E5.20	E6.20
Tâches "Sécurité des Développeurs"		(8a) E2.23+	E3.23	(8b) E4.23	E5.23	E6.23
Tâches "Documentation Utilisateur"	E1.27	(6a) E3.27	E3.27	E4.27	E5.27	E6.27
Tâches "Documentation d'Administration"	E1.30	(6b) E2.30	E3.30	E4.30	E5.30	E6.30
Tâches "Livraison et Configuration"	E1.34	(6c) E2.34+	E3.34	E4.34	E5.34	E6.34
Tâches "Démarrage et Exploitation"	E1.37	(6d) E2.37	E3.37	E4.37	E5.37	E6.37

+ indique une rigueur accrue dans la tâche

indique que la tâche est traitée dans les exemples

(n) **indique que la tâche est traitée dans l'exemple n**

Figure 5.1.2 Tâches de l'évaluateur pour la conformité selon les critères ITSEC (ii)

	E1	E2	E3	E4	E5	E6
Tâches "Pertinence de la Fonctionnalité"	**3.16**	**3.16+**	(7) **3.16+**	**3.16+**	**3.16+**	3.16+
Tâches "Cohésion de la Fonctionnalité"	**3.20**	**3.20+**	(7) **3.20+**	**3.20+**	**3.20+**	**3.20+**
Tâches "Résistance des Mécanismes"	**3.24**	**3.24+**	(7) **3.24+**	**3.24+**	**3.24+**	**3.24+**
Tâches "Estimation de la Vulnérabilité de Construction"	**3.28**	**3.28+**	(7) **3.28+**	**3.28+**	**3.28+**	**3.28+**
Tâches "Facilité d'Emploi"	**3.33**	**3.33+**	(7) **3.33+**	**3.33+**	**3.33+**	**3.33+**
Tâches "Estimation de la Vulnérabilité en Exploitation"	**3.37**	**3.37+**	(7) **3.37+**	**3.37+**	**3.37+**	**3.37+**

+ indique une rigueur accrue dans la tâche

indique que la tâche est traitée dans les exemples

(n) indique que la tâche est traitée dans l'exemple n

Figure 5.1.3 Tâches de l'évaluateur pour l'efficacité selon les critères ITSEC

Chapitre 5.2 Exemple 1, examiner l'environnement de développement (E2 et E4)

Introduction

5.2.1 Cet exemple présente deux sous-exemples (1(a) et 1(b)) qui abordent chacun un aspect de l'environnement de développement à des niveaux d'évaluation différents.

Exemple 1(a) - Sous-activité : examiner la gestion de configuration (E2.17)

Introduction

5.2.2 Ce sous-exemple traite des tâches de l'évaluateur de "L'environnement de développement, Aspect 1 - Gestion de configuration". Les caractéristiques de l'évaluation étaient les suivantes :

a) la cible d'évaluation était un système temps-réel ;

b) le niveau d'évaluation visé était E2 ;

c) l'évaluation était effectuée simultanément au développement du système.

Fournitures de l'évaluation concernées

5.2.3 Les données pour ce travail étaient :

a) la liste de configuration qui identifie la version de la cible d'évaluation pour l'évaluation ;

b) de l'information sur le système de gestion de configuration.

Travail effectué

5.2.4 L'information sur le système de gestion de configuration était contenue dans les procédures de gestion de configuration du projet du développeur. Celles-ci ont été analysées par les évaluateurs (en les lisant et les comprenant). En particulier les évaluateurs ont contrôlé que :

a) la liste de configuration énumérait tous les composants élémentaires à partir desquels la cible d'évaluation a été construite[1];

b) les procédures exigeaient que tous les composants élémentaires et que l'ensemble de la documentation concernée possèdent un identifiant unique et que l'emploi de celui-ci soit obligatoire dans les références[2] ;

c) les procédures exigeaient que la cible d'évaluation soumise soit conforme à la documentation fournie et que seuls les changements autorisés soient possibles[3].

1. NdT: ITSEC E2.15:2.la traduction a été reprise.
2. NdT: ITSEC E2.15:3:4.la traduction n'a pu être reprise (incohérence ITSEC-ITSEM).
3. NdT ITSEC E2.15:5.La traduction a été reprise.

5.2.5 Les évaluateurs ont ensuite pu visiter le site de développement et confirmer que les procédures de gestion de configuration avaient été appliquées par :

a) une estimation de la conformité aux pratiques d'autres documentations fournies ;

b) un entretien avec le personnel pour savoir s'il était au courant des pratiques et s'il pensait qu'elles étaient suivies.

5.2.6 Pour assurer que les pratiques étaient suivies de façon cohérente, les évaluateurs :

a) se sont entretenus séparément avec plusieurs équipes de développement, posant les mêmes questions lors de chaque entretien ;

b) se sont entretenus avec les cadres supérieurs ainsi qu'avec les subalternes : alors que les cadres supérieurs peuvent être mieux informés des pratiques à adopter, les subalternes peuvent traduire une compréhension plus réaliste de ce qui est réellement fait.

5.2.7 Afin de vérifier plus en détail que les procédures décrites étaient appliquées, les évaluateurs ont alors :

a) sélectionné plusieurs objets ;

b) retracé l'historique des changements au moyen du système de gestion de configuration (en vérifiant les aspects tels que : l'autorisation appropriée pour effectuer un changement, les fiches de demande de modification correctement utilisées, etc.).

5.2.8 Étant donné que les critères de conformité des ITSEC concernant la gestion de configuration ont été satisfaits, un verdict de réussite a pu être prononcé.

Exemple 1(b) - Sous-activité : examiner les langages de programmation et les compilateurs (E4.20)

Introduction

5.2.9 Ce sous-exemple traite des tâches de "L'environnement de développement, Aspect 2 - Langages de programmation et compilateurs ".

5.2.10 La cible d'évaluation a été réalisée à l'aide d'un langage de programmation structuré et d'un compilateur du commerce qui possédait des extensions à la norme ISO pour ce langage. Le niveau d'évaluation visé était E4.

Fournitures de l'évaluation concernées

5.2.11 Les données pour ce travail étaient :

a) le manuel de référence du compilateur ;

b) les normes de programmation à utiliser par l'équipe de développement, y compris une définition des options du compilateur devant être utilisées.

Travail effectué

5.2.12 Les fournitures concernant le langage de réalisation et les compilateurs utilisés dans le développement de la cible d'évaluation ont été examinées pour déterminer si le développeur utilisait un langage de programmation parfaitement[1] défini. Les évaluateurs ont noté que le manuel de référence du compilateur ne faisait aucune déclaration à propos de la conformité avec une norme reconnue de ce langage (par exemple, des normes ANSI ou ISO).

5.2.13 Les normes de programmation propres au développeur définissaient un sous-ensemble de déclarations du langage de programmation dérivé de la norme ISO de ce langage. Etant donné que le compilateur n'avait pas été homologué conformément à une quelconque norme reconnue, les évaluateurs ont constaté qu'il était nécessaire d'examiner le manuel de référence de ce compilateur pour vérifier que le sens de toutes les déclarations[2] identifiées dans les normes du développeur était défini sans ambiguïté.

5.2.14 La documentation du compilateur a également été analysée pour vérifier les répercussions des options du compilateur identifiées dans les normes du développeur. Par exemple, certains compilateurs induisent des effets inattendus (tels que l'optimisation par déplacement de code source en dehors des boucles) lorsque l'option OPTIMISATION est sélectionnée.

5.2.15 Les évaluateurs ont noté que le compilateur en question était un produit largement diffusé sur le marché, et que de ce fait il avait été convenablement testé. Les problèmes connus liés au compilateur étaient correctement décrits dans la notice de distribution du compilateur et sont apparus n'avoir aucune conséquence sur le développement de la cible d'évaluation.

5.2.16 Outre la définition d'un sous-ensemble des commandes du langage, les normes de programmation du développeur excluaient l'utilisation de constructions et techniques jugées "non-sûres" par le développeur, à savoir :

a) des branchements calculés inconditionnels (*GOTO*) ;

b) l'introduction de synonymes (*alias*, par exemple, l'instruction *EQUIVALENCE* en Fortran).

5.2.17 Les évaluateurs ont également noté que les normes du développeur imposaient des pratiques de programmation défensives, telles que :

a) l'utilisation de types de données (types énumérés, sous-intervalles, etc.) ;

b) la définition commune de types et variables utilisés par plus d'un composant (par exemple, par l'emploi des déclarations *INCLUDE*) ;

c) le traitement des exceptions : vérification des intervalles et vérification des bornes de tableaux, traitement de la division par zéro et débordement arithmétique ;

d) la vérification globale de type au sein des différentes unités de compilation.

1. NdT : ITSEC E4.18:1 La traduction de l'ITSEC a été reprise.
2. NdT : ITSEC E4.19 La traduction de l'ITSEC a été reprise.

5.2.18 Les évaluateurs ont été capables de confirmer que les normes de programmation du développeur étaient respectées. La vérification du respect des normes du développeur a été effectuée simultanément avec les tâches de l'évaluateur relatives à l'examen du code source faisant partie de l'activité pour examiner la conformité de la réalisation.

5.2.19 Finalement, les évaluateurs ont examiné les "fichiers de construction" ainsi que leur utilisation pour s'assurer que les options du compilateur exigées par les normes de programmation avaient été utilisées tout au long du projet de développement.

5.2.20 En conclusion, les évaluateurs ont été capables de prononcer un verdict *de réussite* pour cet aspect de l'environnement de développement.

Chapitre 5.3 Exemple 2, examiner la conformité de la spécification des besoins (E4)

Introduction

5.3.1 Cet exemple traite des tâches de l'évaluateur de "Construction - Le processus de développement, Phase 1 - Spécification des besoins". La cible d'évaluation était un système spécifique. La cible de sécurité de la cible d'évaluation spécifiait la classe de fonctionnalité F-B1.

Fournitures d'évaluation concernées

5.3.2 La cible de sécurité comprenait :

a) une politique de sécurité système[1] (SSP) ;

b) une politique de sécurité de l'information dans les systèmes électroniques (SEISP) ;

c) un modèle de politique de sécurité (SPM) ;

d) le niveau d'évaluation visé : E4 ;

e) la cotation de la résistance minimum des mécanismes : moyenne ;

f) des mécanismes cryptographiques requis[2].

5.3.3 La relation entre ces différents éléments de la cible de sécurité est décrite dans la figure 5.3.1.

5.3.4 Les SSP, SEISP et SPM étaient cohérents avec la version 1.2 des ITSEC, paragraphes 2.27 à 2.29 inclus.

5.3.5 Le SPM fournissait un modèle formel en notation Z des besoins concernant l'identification, l'**authentification** et le contrôle d'accès pour le système. Le SPM comportait le calcul des pré-conditions et les démonstrations que les transitions d'état étaient sûres. Le SPM fournissait également une interprétation informelle des spécifications des besoins concernant l'identification, l'authentification et le contrôle d'accès formellement définis. Le SPM référençait le modèle de Bell-La Padula de politique de sécurité sous-jacente.

5.3.6 Les fonctions dédiées à la sécurité de la SEISP étaient données pour fournir une interprétation informelle du modèle de politique de sécurité sous l'angle[3] de la cible de sécurité.

1. NdT ITSEC E4.2:2 La traduction a été reprise.
2. NdT ITSEC 2.23. La traduction a été reprise.
3. NdT ITSEC E4.2:5 La traduction a été reprise.

Travail effectué

5.3.7 Les exigences concernant le contenu, la présentation et les éléments de preuves des fournitures concernant la spécification des besoins ont été vérifiées. Les évaluateurs ont constaté que, bien que les spécifications des besoins concernant l'identification, l'authentification et le contrôle d'accès avaient été correctement spécifiées dans un style semi-formel, les spécifications des besoins concernant l'imputabilité, l'audit et la réutilisation d'objet n'avaient été spécifiées que dans un style informel.

5.3.8 Les évaluateurs ont établi un rapport d'anomalie, en recommandant que les spécifications des besoins qui n'avaient pas été présentées dans un style semi-formel pouvaient être décrites au moyen de diagrammes de flots de données, d'une structure de données logique et de séquences de comportement des entités, cohérent avec le style de présentation utilisé pour les spécifications des besoins de sécurité, correctement spécifiées dans un style semi-formel (la méthode structurée d'analyse et de conception de systèmes (SSADM) avait été adoptée pour le projet).

5.3.9 La vérification effectuée par les évaluateurs comprenait :

a) la correspondance entre les fonctions dédiées à la sécurité de la SEISP et les objectifs de sécurité et les menaces à la sécurité identifiés dans la SSP ;

b) la vérification manuelle de la SEISP par rapport à la SSP pour assurer que la documentation était cohérente ;

c) la validation des fonctions dédiées à la sécurité de la SEISP par rapport au SPM formel et le texte s'y rapportantl ;

d) la vérification que le SPM préservait le but du modèle de Bell-La Padula.

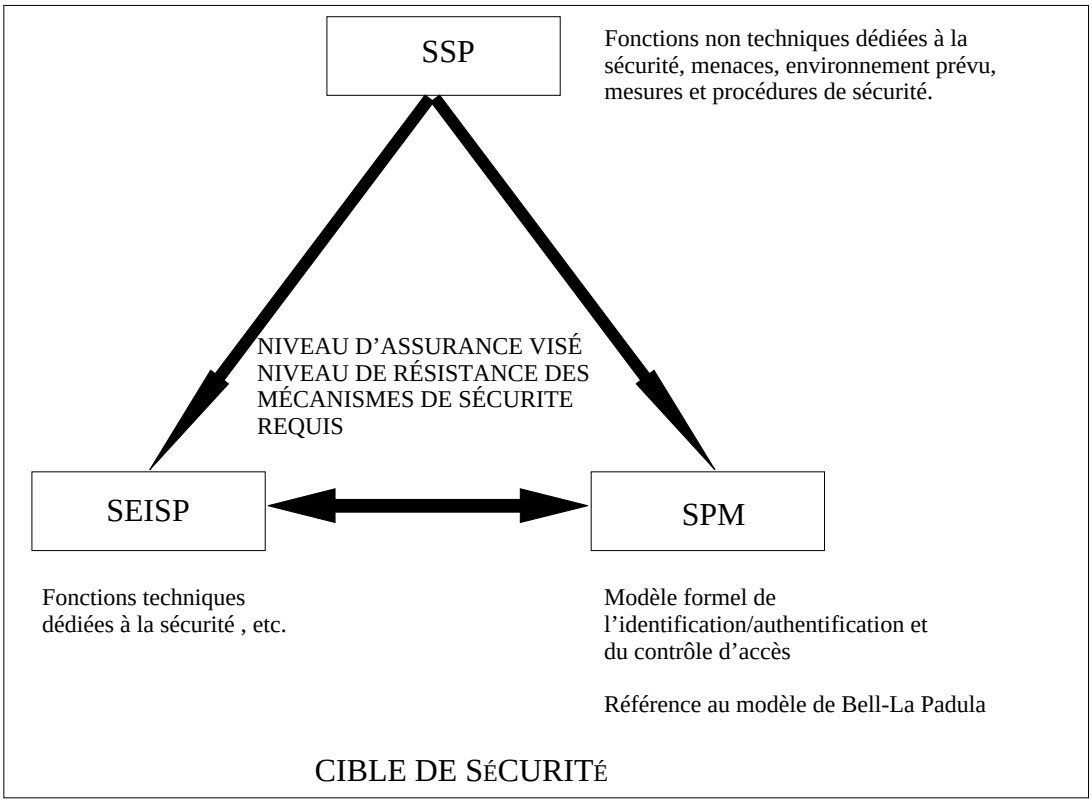
5.3.10 Le SPM a été validé par :

a) la lecture et la compréhension approfondie du document ;

b) la compréhension et la vérification indépendante des preuves des pré-conditions et des démonstrations (pour s'assurer que les transitions d'état étaient réellement sûres) ;

c) la validation du fait que l'état initial était sûr.

5.3.11 Comme les critères de conformité des ITSEC n'étaient pas clairement satisfaits, il fut possible de prononcer un verdict *à confirmer*. Ce verdict *à confirmer* a par la suite été modifié en un verdict *de réussite* lorsque les évaluateurs ont été capable de vérifier la spécification semi-formelle des besoins pour l'imputabilité, l'audit et la réutilisation d'objet fournie par le commanditaire au cours d'une étape ultérieure de l'évaluation.



Légende :
SSP - Politique de Sécurité Système
SEISP - Politique de Sécurité de l'Information dans les Systèmes Electroniques
SPM - Modèle formel de Politique de Sécurité

Figure 5.3.1 Décomposition structurelle de la documentation

Chapitre 5.4 Exemple 3, examiner la conformité de la conception générale (E4)

Introduction

5.4.1 Cet exemple traite des tâches de l'évaluateur de "Construction - Le processus de développement, Phase 2 - Conception générale". La cible d'évaluation était un système réparti qui comportait de nombreux composants et elle avait été développée juste avant la publication des critères ITSEC. Il a été trouvé que la documentation fournie satisfaisait entièrement aux exigences du niveau E4, certaines parties de la documentation étaient conformes aux exigences de niveaux supérieurs. La cible de sécurité de la cible d'évaluation spécifiait la classe de fonctionnalité F-B3 avec certaines fonctionnalités supplémentaires.

Fournitures d'évaluation concernées

5.4.2 Les données pour ce travail étaient la cible de sécurité et la conception générale de la cible d'évaluation.

5.4.3 La figure 5.4.1 fournit une décomposition de la structure de la documentation fournie aux évaluateurs par les développeurs. Les évaluateurs ont identifié les parties de la documentation qui contenaient la conception générale. La conception générale est décrite en figure 5.4.1.

5.4.4 La conception générale comprenait :

a) une spécification fonctionnelle du système (SFS) ;

b) une spécification formelle de sécurité (FSS) ;

c) un dossier d'architecture de la sécurité (SAD).

5.4.5 La cible d'évaluation avait été développée à l'aide de SSADM. La SFS comportait les produits des étapes 1 à 3 de SSADM. Les résultats de SSADM étaient les suivants :

a) les diagrammes de flots de données (DFD) ;

b) les descriptions des processus associés aux DFD ;

c) les descriptions des entités externes (sur les DFD) ;

d) un catalogue des entrées/sorties ;

e) une structure de données logique (LDS) ;

f) les descriptions des entités ;

g) un inventaire des données ;

h) des références croisées entre entités et fichiers ;

i) un catalogue des événements ;

j) une matrice événement/entité ;

k) les diagrammes des séquences de comportement des entités (ELH).

5.4.6 La SFS fournissait la conception logique, qui rassemblait les exigences fonctionnelles issues de la spécification de besoins du système (SRS) et de la politique de sécurité de l'information dans les systèmes électroniques (SEISP). Une partie de la SFS, l'interface logique Homme-Machine (MMI), présentait ce que les utilisateurs du système voient (au moyen de diagrammes de transition d'état) pour tous les types d'utilisateurs. La SFS n'imposait rien qui concernait les aspects physiques de la MMI tel que la disposition à l'écran.

5.4.7 Une partie de la SFS, les spécifications des interfaces externes (EIS), définissait les interfaces externes (pour des systèmes externes et les systèmes embarqués existants). Les EIS présentaient les systèmes externes et embarqués à connecter au réseau du système et donnaient des détails sur les interfaces de communication. Les fonctions dédiées à la sécurité qui concernait les interfaces de communication étaient explicitement identifiées.

5.4.8 On remarquera que les MMI et EIS constituaient des documents distincts. Toutefois, pour l'évaluation, ils ont été considérés comme une partie de la spécification fonctionnelle du système.

5.4.9 La FSS comprenait une spécification formelle rédigée en 'Z', détaillant un sous- ensemble des fonctions dédiées à la sécurité, à savoir le contrôle d'accès obligatoire, l'imputabilité et l'audit. La spécification comprenait un développement textuel de ce sous-ensemble. Il existait une correspondance entre la SFS et la FSS. Bien que ce ne soit pas une exigence au niveau E4, la FSS a été utilisée pour déterminer les événements spécifiés dans la SFS qui étaient touchant à la sécurité.

5.4.10 Le SAD fournissait un aperçu de la configuration de la cible d'évaluation considérée, ainsi que des descriptions de haut niveau sur la façon dont la politique de sécurité devait être implémentée dans le contexte de cette configuration. Il fournissait une description sur la façon dont les fonctions dédiées à la sécurité pourraient être satisfaites. Il décrivait comment les exigences de séparation pouraient être satisfaites.

5.4.11 Le SAD spécifiait les pratiques et les procédures à suivre pour la conception détaillée et le cycle de vie du développement vis-à-vis des parties dédiées à la sécurité, des parties touchant à la sécurité et des parties ne touchant pas à la sécurité de la cible d'évaluation, telles que :

a) les procédures de qualité ;

b) les méthodes de conception détaillée ;

c) les procédures de documentation de la traçabilité ;

d) les tests fonctionnels ;

e) la gestion de configuration ;

f) le contrôle des changements.

5.4.12 Ces éléments ont été extraits et utilisés comme donnée pour d'autres activités de l'évaluation (qui ne font pas partie de cet exemple), telles que :

a) la conception détaillée (alinéa (b), comme information de contexte) ;

b) la réalisation (alinéa (d), car elle décrivait la stratégie de test à entreprendre et, en particulier, présentait les mesures de couverture de test à effectuer et justifiait pourquoi la couverture serait suffisante) ;

c) La gestion de configuration (alinéas (a), (c), (e) et (f) qui expliquaient le système de gestion de configuration dans le contexte global des procédures de gestion de la qualité, identifiaient et expliquaient l'utilisation des outils de gestion de configuration, les procédures de recette et l'autorité de référence qui permet d'effectuer des changements).

5.4.13 L'un des composants du système était une station de travail dédiée à la sécurité et touchant à la sécurité. Le SAD fournissait :

a) une vue d'ensemble de l'architecture de la station de travail ;

b) l'identification des composants dédiés à la sécurité (tels que l'interface du réseau) et des composants touchant à la sécurité.

5.4.14 Les fonctions dédiées à la sécurité étaient référencées dans les SEISP, SFS (descriptions des processus) et FSS (développement textuel). Les références étaient liées dans des documents de traçabilité distincts, qui fournissaient :

a) une traçabilité ascendante à partir des fonctions dédiées à la sécurité de la SEISP vers les fonctions des SFS et FSS ;

b) une traçabilité descendante à partir des fonctionnalités des SFS et FSS vers les fonctions dédiées à la sécurité de la SEISP.

5.4.15 Les documents de traçabilité fournissaient des justifications qui concernaient les instructions non traçables dans les SFS et FSS.

Travail effectué

5.4.16 Toutes les fournitures au niveau de la conception générale ont été examinées pour vérifier que les exigences des critères ITSEC concernant le contenu, la présentation et les éléments de preuve avaient été satisfaites. Il a notamment été vérifié que :

a) toutes les interfaces externes prévues avaient été identifiées et que les mécanismes de séparation temporelle et les mécanismes cryptographiques appropriés avaient été pris en considération (dans les EIS et le SAD) ;

b) tous les composants matériels et microprogrammés avaient été identifiés et que la fonctionnalité des mécanismes de protection de soutien était appropriée. Par exemple, que la station de travail fournirait des mesures adéquates pour la réutilisation d'objet pour toute la mémoire (dans le SAD) ;

c) la séparation entre les composants dédiés à la sécurité, les composants touchant à la sécurité et les composants ne touchant pas à la sécurité était réalisable et judicieuse (dans le SAD et la SFS).

5.4.17 Des procédures de documentation SSADM spécifiques au projet ont été adoptées. Les procédures spécifiques au projet ont été examinées pour assurer que les évaluateurs comprenaient clairement la syntaxe et la sémantique de la notation semi-formelle. La SFS a été comparée aux normes de documentation pour assurer que les procédures du projet étaient correctement suivies.

5.4.18 La vérification des éléments de preuve de la traçabilité impliquait une vérification manuelle des SFS et FSS par rapport à la SEISP. La vérification portait sur l'introduction des fonctionnalités non traçables, assurant que la justification de ces fonctionnalités était adéquate.

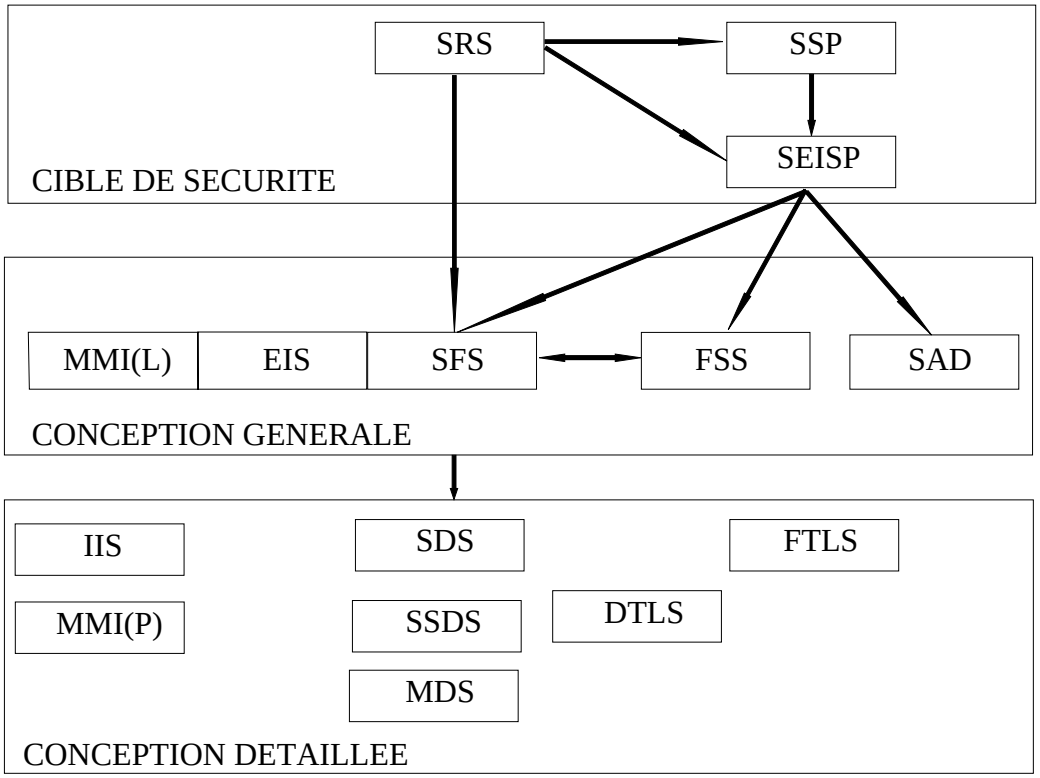
5.4.19 Les évaluateurs ont constaté que la documentation SSADM dans la SFS ne séparait pas logiquement les fonctions dédiées à la sécurité, les fonctions touchant à la sécurité et les autres fonctionnalités, et ont établi un rapport d'anomalie. Le commanditaire a pris en considération la question et a engagé un consultant, indépendant de cette évaluation, afin qu'il recommande une approche pratique qui permette de résoudre le problème.

5.4.20 Les consultants en sécurité ont identifié le fait que les événements décrits dans le catalogue des événements n'avaient pas été classés dans les catégories "touchant à la sécurité" ni "ne touchant pas à la sécurité". En considérant à la fois la FSS et les causes des événements, le consultant a pu décider quels événements étaient dédiés à la sécurité.

5.4.21 Le consultant a recommandé une meilleure approche, que le développeur aurait pu adopter, qui aurait été d'identifier la fonctionnalité de sécurité à un processus associé au DFD de plus haut niveau. Ce processus aurait alors pu être raffiné en fonctions dédiées à la sécurité (telles que le contrôle d'accès, l'imputabilité, etc.) et aurait fourni une séparation logique et claire de la fonctionnalité, ainsi qu'une indication précise de l'indépendance des composants dédiés à la sécurité. Cependant, le consultant a précisé qu'au niveau E4, l'utilisation de SSADM dans la SFS était rigoureusement correcte et, que si tous les processus DFD de niveau inférieur étaient classés comme "dédiés à la sécurité" ou "non dédiés à la sécurité", le document SAD décrirait une séparation physique suffisante pour que la conception générale satisfasse aux exigences des critères d'évaluation.

5.4.22 Cet argument a été accepté par les évaluateurs. La catégorisation des processus était alors fournie au CESTI, permettant la poursuite de l'évaluation.

5.4.23 Étant donné que les critères de conformité des ITSEC pour la conception générale étaient satisfaits, il fut possible de prononcer un verdict *de réussite*.



Légende:
SRS - Spécifications des Besoins du Système
SSP - Politique de Sécurité du Système
SEISP - Politique de Sécurité de l'Information dans les Systèmes Electroniques
SFS - Spécifications Fonctionnelles du Système (SSADM 1-3)
IIS/EIS - Spécifications d'Interface Interne/Externe
MMI(L) - Interface Homme-Machine (Logique)
FSS - Spécification Formelle de la Sécurité
SAD - Dossier d'Architecture du Système
MMI(P) - Interface Homme-Machine (Physique)
SDS, SSDS, MDS, FTLS, DTLS - Conception Détaillée

Figure 5.4.1 Décomposition structurelle de la documentation

Chapitre 5.5 Exemple 4, examiner la conformité de la conception détaillée (E2)

Introduction

5.5.1 Cet exemple traite des tâches de l'évaluateur de "Construction - Le processus de développement, phase 3 - Conception détaillée". La cible d'évaluation était un système spécifique. La cible de sécurité de la cible d'évaluation spécifiait la classe de fonctionnalité F-DI.

5.5.2 L'évaluation devait être effectuée simultanément au développement du système et, par conséquent, la plupart des fournitures n'étaient initialement disponibles que sous une forme provisoire. Préalablement à l'évaluation, un contrat avait été passé avec un CESTI pour que ce dernier révise les documents provisoires afin de déterminer s'ils pouvaient satisfaire aux exigences du niveau E2.

5.5.3 Il apparut clairement dans l'analyse initiale qu'il y avait de nombreuses zones pour lesquelles la cible d'évaluation ne pourrait atteindre le niveau d'évaluation visé. Le commanditaire fut alors averti des mesures qui devaient être prises pour assurer la réussite de l'évaluation.

Fournitures d'évaluation concernées

5.5.4 Les données pour ce travail étaient la documentation de la conception générale (conception niveau 1) et la documentation de la conception détaillée pour la cible d'évaluation.

5.5.5 La documentation de la conception détaillée contenait :

a) les spécifications de conception des sous-systèmes (conception de niveau 2) ;

b) les spécifications des interfaces des sous-systèmes (conception de niveau 2) ;

c) les spécifications de réalisation (conception de niveau 3).

Travail effectué

5.5.6 La structure des niveaux de **représentation** de la cible d'évaluation a été estimée en fonction des critères en vue d'une relation claire et hiérarchique. Il a été constaté que les spécifications des interfaces des sous-systèmes étaient produites sous la forme d'un document de conception de niveau 2, mais qu'elles contenaient des informations provenant des travaux de conception de niveau 3. Cependant, bien que la présentation des informations n'ait pas été conforme au critère du niveau d'évaluation, le contenu des informations fut considéré comme étant approprié.

5.5.7 La correspondance entre les fonctions dédiées à la sécurité identifiées dans la documentation de la conception générale et les fonctions présentées dans les spécifications de conception des sous-systèmes a été vérifiée manuellement au moyen de références croisées pour assurer que :

a) toutes les fonctions dédiées à la sécurité étaient comprises dans la conception détaillée ;

b) la conception détaillée préservait convenablement l'objectif de la conception générale.

5.5.8 Une matrice de traçabilité des exigences a été produite pour vérifier le lien[1] entre les fonctions dédiées à la sécurité et touchant à la sécurité présentées dans les spécifications de conception des sous-systèmes et les composants dédiés à la sécurité et touchant à la sécurité des spécifications de réalisation. Certaines erreurs ont été relevées, en particulier :

a) certains composants des spécifications de réalisation identifiés par les évaluateurs comme touchant à la sécurité n'étaient pas présentés dans les spécifications de conception des sous-systèmes (i.e. l'absence d'une fonctionnalité touchant à la sécurité dans les représentations de niveau supérieur) ;

b) certaines fonctions dédiées à la sécurité présentées dans les spécifications de conception des sous-systèmes (par exemple, la réutilisation d'objet) n'étaient pas incluses dans les spécifications de la réalisation.

5.5.9 Les spécifications de tous les composants et mécanismes dédiés à la sécurité ou touchant à la sécurité ont été vérifiées pour assurer qu'elles étaient convenablement documentées. Il est apparu que les informations nécessaires pour réaliser les composants dédiés à la sécurité et touchant à la sécurité n'étaient pas toujours fournies. Par exemple :

a) un niveau de détail insuffisant pour l'utilisation et le contenu des structures de données clefs et sur les actions à entreprendre en cas d'échec de la validation d'un paramètre ;

b) des références externes manquantes (par exemple, l'identification des bibliothèques et des composants externes du système utilisés) ;

c) des descriptions en langage naturel de fonctions touchant à la sécurité incohérentes avec les descriptions du pseudo-code qui correspondait.

5.5.10 Les interfaces pour les composants dédiés à la sécurité et touchant à la sécurité ont fait l'objet d'une vérification par recoupement manuel avec les documents de spécifications des interfaces des sous-systèmes pour assurer que toutes les interfaces étaient identifiées et correctement spécifiées. Les erreurs étaient particulièrement importantes car les documents de spécifications des interfaces du système constituaient le guide définitif de programmation pour les fonctions dédiées à la sécurité et des fonctions touchant à la sécurité.

5.5.11 Les exemples ci-dessus dans lesquels les représentations de la conception détaillée de la cible d'évaluation n'étaient pas conformes aux critères du niveau d'évaluation résultaient principalement d'avoir évaluer la cible d'évaluation aux travers de représentations provisoires. Cependant, les évaluateurs ont également reconnu que la conception détaillée n'avait pas été produite de façon à être pleinement conforme aux exigences du niveau E2 et des rapports d'anomalie ont été soumis par les évaluateurs.

1. NdT : ITSEC E2.8:3.La traduction a été reprise.

5.5.12 Les évaluateurs ont été incapables de prononcer un verdict *de réussite* pour la conception détaillée à ce stade de l'évaluation. Un verdict *à confirmer* a été prononcé car les évaluateurs examinaient des représentations provisoires de la cible d'évaluation.

5.5.13 Les versions définitives des représentations de la conception détaillée ont été réexaminées avant l'achèvement de l'évaluation et les problèmes mentionnés se sont avérés résolus. Un verdict *de réussite* fut alors prononcé.

Chapitre 5.6 Exemple 5, examiner la conformité de la réalisation (E2)

Introduction

5.6.1 Cet exemple traite des tâches de l'évaluateur de "Construction - Le processus de développement, phase 4 - Réalisation".

5.6.2 La cible d'évaluation était un système spécifique. La cible de sécurité de la cible d'évaluation spécifiait une classe de fonctionnalité F-DI.

Fournitures d'évaluation concernées

5.6.3 Les données pour ce travail étaient :

a) la documentation de test :

- spécifications des tests de paquetage[1] ;
- plan des tests de recette ;
- spécification des tests des interfaces ;
- spécification des tests de recette du système ;
- spécification des tests de recette des fonctions du système ;
- planification des tests ;
- fichiers de résultats des tests ;
- description des outils de test et du guide de l'utilisateur ;

b) une bibliothèque de programmes d'essai et d'outils qui ont été utilisés par les développeurs pour tester la cible d'évaluation.

5.6.4 Le test de la cible d'évaluation a été effectué en deux phases :

a) tests de paquetage ;

b) tests de recette.

5.6.5 Les tests de recette comprenaient les étapes suivantes :

a) test des interfaces : vérifier que les composants intégrés s'exécutent comme spécifié dans la conception et que l'intégrité des données partagées est maintenue ;

1. NdT ITSEC 6.64.La traduction a été reprise.

b) tests fonctionnels : vérifier que les composants intégrés fournissent un service du système tel que spécifié dans la conception et que les spécifications des besoins des utilisateurs ont été satisfaits ;

c) tests du système : une intégration totale des matériels et des logiciels pour vérifier que le système dans son ensemble exécute les fonctions conformément à la conception du système et qu'il satisfait les spécifications des besoins des utilisateurs.

Travail effectué

5.6.6 La conformité de la réalisation de la cible d'évaluation a été estimée selon les critères du niveau E2 en effectuant les actions suivantes pour chaque phase et pour chaque étape des tests identifiées précédemment :

a) passer en revue la documentation de test ;

b) assister aux tests ;

c) passer en revue les rapports de test ;

d) répéter des tests sélectionnés.

5.6.7 La stratégie de test du développeur pour la cible d'évaluation démontrait une approche descendante contrôlée, couvrant toutes les fonctions dédiées à la sécurité identifiées dans la cible de sécurité. Le niveau de test le plus bas auquel ont été soumis les composants de la cible d'évaluation était celui du test de paquetage (un paquetage étant une collection de modules fournissant un ensemble lié de services) et non celui du test unitaire des modules. Toutefois, ceci est suffisant au niveau E2, car il est seulement nécessaire de démontrer que les *tests couvrent toutes les fonctions dédiées à la sécurité...*

5.6.8 L'objectif du développeur pour les tests des paquetages était de tester tous les enchaînements fonctionnels identifiés dans la conception du paquetage avec suffisamment de tests (confirmé par l'utilisation d'un test "en ligne", mis directement dans le code, qui peut être sélectionné au moment de la compilation) pour fournir une couverture complète des lignes de code. Néanmoins, l'estimation des tests d'intégration a révélé que cet objectif n'avait pas été atteint.

5.6.9 La documentation du test de recette contenait des descriptions détaillées de chaque test, incluant l'objectif, les procédures et les ressources.

5.6.10 Le plan de test de recette fournissait une **m**atrice de **t**raçabilité des **b**esoins (MTB) de haut niveau exprimés qui faisait correspondre les phases de test aux spécifications des besoins des utilisateurs. Une MTB plus détaillée a été fournie avec chacune des spécifications de test de recette. Les MTB ont été vérifiées manuellement pour s'assurer que toutes les fonctions dédiées à la sécurité étaient convenablement couvertes. Il a été noté que les MTB étaient incomplètes.

5.6.11 Les évaluateurs ont assisté aux tests de recette pour certaines des fonctions dédiées à la sécurité pour assurer que les procédures de test étaient suivies. Ceci comprenait aussi la demande que des tests achevés précédemment soient répétés.

5.6.12 Les rapports de test de recette ont été passés en revue pour assurer que chaque test avait été achevé avec succès et pour identifier toute faiblesse dans le développement de la cible d'évaluation. Les problèmes fréquemment rencontrés ont été les suivants :

a) les modules de réalisation qui avaient (apparemment) satisfait aux tests de paquetage n'ont pas pu être recompilés au cours des étapes de test ultérieures ;

b) une couverture de test inadéquate lors des tests de paquetage a conduit à des échecs au cours des étapes de test ultérieures ;

c) des effondrements du système se sont produits avec des codes d'erreur non définis.

5.6.13 Ces problèmes ont révélé des faiblesses dans le processus de développement. Les évaluateurs ont établi un seul rapport d'anomalie pour couvrir tous ces points. Le développeur a été capable de démontrer par la suite que ces questions avaient été traitées.

5.6.14 Des tests supplémentaires ont été identifiés par les évaluateurs pour rechercher des erreurs mais, compte-tenu de la complexité des programmes de test, il ne leur a pas été possible de les exécuter eux-mêmes. Pour passer outre ce problème, le développeur a reçu les spécifications de test concernant les tests supplémentaires à effectuer. Les évaluateurs ont alors assisté à ces tests.

5.6.15 Comme les critères de conformité des ITSEC pour la réalisation étaient satisfaits, il a été possible de prononcer un verdict *de réussite*.

Chapitre 5.7 Exemple 6, examiner la conformité de l'exploitation (E2)

Introduction

5.7.1 Cet exemple présente quatre sous-exemples (6(a), 6(b), 6(c) et 6(d)), chacun d'eux aborde un aspect de la documentation d'exploitation ou de l'environnement d'exploitation.

Exemple 6(a) - Sous-activité : examiner la documentation utilisateur (E2.27)

Introduction

5.7.2 Ce sous-exemple traite des tâches de l'évaluateur de "Documentation d'exploitation, aspect 1 - Documentation utilisateur". La cible d'évaluation était un système. La cible de sécurité de la cible d'évaluation spécifiait la classe de fonctionnalité F-C2.

5.7.3 La sous-section *Rigueur et degré d'approfondissement des éléments de preuve* à la fin de cet exemple interprète les transitions en terme de rigueur dans la documentation utilisateur lorsque l'on passe de *présenter* à *décrire* puis à *expliquer*.

Fournitures d'évaluation concernées

5.7.4 Les données pour ce travail étaient la cible de sécurité et l'ensemble des guides de l'utilisateur de la cible d'évaluation.

Travail effectué

5.7.5 Les guides de l'utilisateur ont été mis en correspondance avec les fonctions dédiées à la sécurité de la cible de sécurité pour assurer une couverture complète et cohérente des fonctions dédiées à la sécurité qui concernent l'utilisateur final. Des fonctions d'administration, telles que l'audit, n'ont pas été considérées pertinentes.

5.7.6 Les évaluateurs ont visité le site à plusieurs reprises. Ils ont ainsi pu acquérir une bonne compréhension de la façon dont le système fonctionnait. L'utilisation du système a pu alors être comparée aux descriptions des guides de l'utilisateur (afin d'estimer leur conformité) et les doutes résiduels des guides de l'utilisateur quant à l'intention ont pu être clarifiés.

5.7.7 Les guides de l'utilisateur présentaient comment les menus du système pouvaient être utilisés. Les menus du système ont été vérifiés pour assurer qu'ils correspondaient correctement aux guides de l'utilisateur.

5.7.8 Les guides de l'utilisateur ont été passés en revue de manière approfondie par les évaluateurs pour assurer que les faiblesses possibles de la sécurité n'étaient pas présentées aux utilisateurs.

Rigueur et qualité des éléments de preuve - Introduction

5.7.9 Cette sous-section fournit un exemple de la façon dont les exigences concernant le contenu, la présentation et les éléments de preuve changent selon les niveaux lorsque les verbes présenter, décrire et expliquer sont utilisés dans les critères ITSEC,en en indiquant des points positifs et négatifs. L'exemple choisi met en garde contre les dangers qu'il y a à ne pas prendre en compte le contexte lors de l'interprétation de ce concept ITSEC.

5.7.10 Les changements suivants dans les exigences concernant le contenu, la présentation et les éléments de preuve de la documentation utilisateur sont détaillés dans les critères ITSEC :

a) Pour E1 et E2, *la documentation utilisateur doit **présenter** les fonctions dédiées à la sécurité qui concernent l'utilisateur final* et *la documentation utilisateur doit **présenter** comment un utilisateur final utilise*[1] *la TOE de façon sûre*.

b) Pour E3 et E4, *la documentation utilisateur doit **décrire** les fonctions dédiées à la sécurité qui concernent l'utilisateur final* et *la documentation utilisateur doit **décrire** comment un utilisateur final utilise la TOE de façon sûre*.

c) Pour E5 et E6, *la documentation utilisateur doit **expliquer** les fonctions dédiées à la sécurité qui concernent l'utilisateur final* et *la documentation utilisateur doit **expliquer** comment un utilisateur final utilise la TOE de façon sûre*.

5.7.11 Le paragraphe 0.12 des critères ITSEC[2] définit les verbes présenter, décrire et expliquer comme suit. *Présenter signifie que les éléments pertinents doivent être fournis ; décrire signifie que ces éléments doivent être fournis et leurs caractéristiques pertinentes énumérées ; expliquer signifie que ces éléments doivent être fournis, leurs caractéristiques pertinentes énumérées et des justifications données*.

5.7.12 Le volume de l'effort nécessaire pour vérifier que les informations fournies satisfont à toutes les exigences concernant le contenu, la présentation et les éléments de preuve varient donc avec le niveau d'évaluation.

5.7.13 La cible de sécurité pour un système pourrait spécifier une fonction dédiée à la sécurité pour limiter les tentatives de connexion sur un terminal. Dans ce cas, les besoins pourraient s'exprimer ainsi :

a) le système ne doit pas autoriser plus de trois échecs de connexion consécutifs ;

b) si trois échecs de connexion consécutifs se produisent, alors l'écran doit être effacé et le clavier doit être verrouillé ;

c) le système doit enregistrer tous les échecs de connexion.

5.7.14 L'effet des différents niveaux d'évaluation est discuté ci-après.

1. NdT : ITSEC E2.26.Le temps est celui de la traduction.
2. NdT : ITSEC 0.12.La traduction a été reprise.

Interprétation pour E1 et E2

5.7.15 Pour E1 et E2, les guides de l'utilisateur pourraient présenter qu'un utilisateur ne dispose que de trois tentatives pour se connecter d'un terminal et qu'après trois échecs, l'écran est effacé, que le clavier est verrouillé et que chaque échec est enregistré par le système. Il s'agit là d'une interprétation raisonnable pour E1 et E2.

5.7.16 Le travail effectué pour E1 et E2 devrait être tel que détaillé dans la sous-section *Travail effectué* ci-dessus.

Interprétation pour E3 et E4

5.7.17 Pour E3 et E4, les guides de l'utilisateur pourraient décrire qu'un utilisateur ne dispose que de trois tentatives pour se connecter et qu'après trois échecs le processus de connexion :

a) efface l'écran en envoyant (par exemple) une séquence de contrôle ;

b) verrouille le clavier en invalidant l'enregistrement de sa description dans le fichier de configuration du terminal et met à jour sa table interne des terminaux (par exemple) ;

c) écrit un message dans la **trace d'audit** qui identifie le niveau d'incident, la date, l'heure, le type d'incident (i.e. un échec de connexion), l'identifiant du terminal et le nom utilisateur entré. Un exemple de message serait :

" WARNING: 12/08/91: 0935: LOGON FAILURE ON TTY03 BY J_SMITH ".

5.7.18 Dans ce cas, les évaluateurs devraient indiquer que les alinéas (a) et (b) contiennent des détails concernant la réalisation, qui n'ont pas à figurer dans la documentation d'exploitation. L'alinéa (c) contient des détails qui n'ont pas à figurer dans un guide de l'utilisateur, bien qu'il puisse constituer une *description* adéquate pour un guide de l'administrateur.

5.7.19 A la place, le guide de l'utilisateur devrait décrire le processus de connexion et ce qui s'en suit. Par exemple :

a) pour se connecter au système, un utilisateur doit d'abord solliciter le système d'exploitation en appuyant sur une touche quelconque ;

b) le système demandera alors le nom de l'utilisateur, lequel sera affiché ;

c) le système demandera alors le mot de passe de l'utilisateur. Celui-ci ne sera pas affiché ;

d) si le nom de l'utilisateur et le mot de passe ne forment pas une combinaison valide, le système affichera le message "ERROR: PLEASE TRY AGAIN" ;

e) le système demandera alors à nouveau le nom de l'utilisateur (étape (b)). Trois tentatives sont autorisées. Si l'utilisateur échoue à la troisième tentative, l'écran sera effacé et le clavier sera verrouillé. Le terminal ne pourra pas être utilisé pendant une période de cinq minutes (ou tout autre définie par l'administrateur du système) ;

f) si la connexion est réussie, le système affichera alors le menu de commandes de l'utilisateur.

Interprétation pour E5 et E6

5.7.20 Pour E5 et E6, en sus des éléments précédents, les guides de l'utilisateur pourraient expliquer :

a) l'effacement de l'écran donne l'impression d'un dysfonctionnement, de façon à ce que le pirate ne puisse obtenir davantage d'informations ;

b) le verrouillage du clavier empêche le pirate d'essayer d'autres mots de passe ;

c) l'audit des événements avertit l'administrateur qu'un terminal particulier est attaqué (ainsi qu'un compte utilisateur particulier, éventuellement).

5.7.21 A nouveau, les évaluateurs devraient signaler que ces informations n'ont pas à figurer dans un guide de l'utilisateur, bien qu'il fournisse à un administrateur de la sécurité les justifications du développeur. De plus, il faudrait remarquer que cet exemple pourrait également faire l'objet de critiques dans la mesure où il fournit des informations utiles à un attaquant potentiel.

5.7.22 Le paragraphe 5.7.19 constitue un point de départ utile pour expliquer le processus de connexion. En complément, un paragraphe dans l'esprit des lignes ci-dessous est requis :

> *Le but d'une telle connexion est de donner l'assurance au système que vous êtes celui que vous prétendez être, notamment en sorte que personne d'autre ne puisse se connecter au système et se faire passer pour vous. Trois tentatives de connexion sont autorisées pour que vous puissiez commettre une erreur en toute honnêteté lorsque vous entrez votre mot de passe, mais pour empêcher un utilisateur non autorisé de tenter découvrir de façon systématique votre mot de passe. Un échec de connexion en trois tentatives sera automatiquement porté à l'attention de l'administrateur du système.*

5.7.23 Outre le travail effectué pour E3 et E4, les justifications fournies seraient également vérifiées par rapport aux explications de la cible de sécurité concernant les objectifs de sécurité, les menaces et les fonctions dédiées à la sécurité.

5.7.24 Il faudrait noter que, selon le public ciblé pour le guide de l'utilisateur, les développeurs pourraient fournir davantage de détails qu'il n'en est exigé par les critères ITSEC. Par exemple, les développeurs peuvent expliquer au niveau E1 certains aspects à l'attention des utilisateurs inexpérimentés ; ceci peut être une condition d'un contrat de développement.

Exemple 6(b) - Sous-activité : examiner la documentation d'administration (E2.30)

Introduction

5.7.25 Ce sous-exemple traite des tâches de l'évaluateur de "Documentation d'exploitation, aspect 2 - Documentation d'administration". La cible d'évaluation était un système. La cible de sécurité de la cible d'évaluation spécifiait la classe de fonctionnalité F-C2.

Fournitures d'évaluation concernées

5.7.26 Les données pour ce travail étaient la cible de sécurité et l'ensemble des guides de l'administrateur de la cible d'évaluation.

Travail effectué

5.7.27 Les guides de l'administrateur ont été mis en correspondance avec les fonctions dédiées à la sécurité de la cible de sécurité pour assurer une couverture complète et cohérente des fonctions dédiées à la sécurité qui concernent l'administrateur du système.

5.7.28 Au cours des visites du site (voir le paragraphe 5.7.6) les évaluateurs ont appris comment le système pouvait être administré par l'administrateur du système. L'exploitation du système a pu alors être comparée aux descriptions des guides de l'administrateur (pour estimer leur conformité) et les doutes résiduels des guides de l'administrateur quant à l'intention ont pu être éclaircis.

5.7.29 Pour ce système particulier, la faculté de l'administrateur d'accéder aux informations des utilisateurs était sévèrement restreinte. Par conséquent, l'objet principal de ce travail était d'assurer que les procédures qui contrôlent les paramètres de sécurité avaient été suffisamment détaillées.

5.7.30 Une description insuffisante a été mise en évidence dans le domaine de la configuration de l'audit. Les procédures pour l'installation du système permettaient que les mécanismes d'audit soient désinstallés. La cible de sécurité spécifiait des fonctions d'audit dédiées à la sécurité et, par conséquent, les évaluateurs ont établi un rapport d'anomalie pour s'assurer que la documentation d'administration fut modifiée pour indiquer que les mécanismes d'audit doivent être configurés pour opérer dans le système.

5.7.31 Les procédures qui détaillent les mécanismes d'identification et d'authentification ont été passées au crible pour assurer que :

a) les procédures pour gérer les cartes d'identification personnelles étaient cohérentes ;

b) les comptes des utilisateurs devaient être définis avec un nom d'utilisateur unique.

5.7.32 Les procédures qui concernent la gestion propre au matériel de sauvegarde et d'archivage ont été vérifiées. Un rapport d'anomalie a été établi concernant la maintenance sur site de tout le matériel de sauvegarde et d'archivage.

Exemple 6(c) - Sous-activité : examiner la livraison et de la configuration (E2.34)

Introduction

5.7.33 Ce sous-exemple traite des tâches de l'évaluateur de "L'environnement d'exploitation, aspect 1 - Livraison et configuration". La cible d'évaluation était un système. La cible de sécurité de la cible d'évaluation spécifiait la classe de fonctionnalité F-B1.

Fournitures d'évaluation concernées

5.7.34 Les données pour ce travail étaient la cible de sécurité et l'ensemble des pratiques de livraison et de configuration de la cible d'évaluation.

Travail effectué

5.7.35 Les procédures de livraison étaient acceptables dans la mesure où elles se conformaient aux indications publiées par le **schéma national**.

5.7.36 Chaque configuration possible, qui était identifiée dans les procédures, a été vérifiée pour s'assurer qu'elle ne compromettait pas la cible de sécurité.

5.7.37 Une visite sur le site a été réalisée par les évaluateurs pour assister à l'installation du système. Assister à la génération du système a permis d'assurer le respect des procédures documentées et la vérification de la trace d'audit a permis d'assurer que la trace enregistrait de manière exacte la génération réelle du système.

5.7.38 Comme les critères de conformité des ITSEC qui concernent la livraison et la configuration étaient satisfaits, il a été possible de prononcer un verdict *de réussite*.

Exemple 6(d) - Sous-activité : examimer le démarrage et l'exploitation (E2.37)

Introduction

5.7.39 Ce sous-exemple traite des tâches de l'évaluateur de "L'environnement d'exploitation, aspect 2 - Démarrage et exploitation". La cible d'évaluation était un système. La cible de sécurité de la cible d'évaluation spécifiait la classe de fonctionnalité F-C2.

Fournitures d'évaluation concernées

5.7.40 Les données pour ce travail étaient la cible de sécurité et l'ensemble des pratiques de démarrage sûr et d'exploitation de la cible d'évaluation.

Travail effectué

5.7.41 Au cours des visites sur site (voir le paragraphe 5.7.6), les évaluateurs ont appris comment le système était démarré et exploité. L'exploitation du système a pu alors être comparée aux descriptions des pratiques (pour estimer leur conformité) et les doutes résiduels au sujet des objectifs de ces pratiques ont pu être éclaircis.

5.7.42 Aucun exemple de résultats des procédures d'auto-test pour les composants matériels dédiés à la sécurité n'a été mis à la disposition des évaluateurs. Un exemple de composant matériel dédié à la sécurité était un filtre matériel qui liait un identifieur de terminal au réseau. Au cours des visites sur site, les procédures d'auto-test ont relevé un problème matériel de l'équipement, ce qui a permis aux évaluateurs d'avoir une certaine confiance dans les auto-tests.

5.7.43 Des fonctions dédiées à la sécurité d'imputation du démarrage existaient. Par conséquent, le commanditaire a fourni des exemples de traces d'audit créées au cours du démarrage et de l'exploitation. Ces traces ont été vérifiées par rapport à des démarrages effectifs pour assurer une correspondance correcte. Les tests fonctionnels ont été scrutés et ont fourni une bonne couverture des fonctions dédiées à la sécurité.

5.7.44 Les pratiques ont été sérieusement examinées par les évaluateurs pour assurer que d'éventuelles faiblesses de la sécurité n'étaient pas introduites sous la forme d'options de démarrage. Les pratiques ne fournissaient pas de considérations spéciales concernant :

a) l'accès de la salle machine ;

b) la sortie d'une console.

5.7.45 Les procédures pour gérer la sortie non marquée d'une console n'étaient pas décrites et un rapport d'anomalie a donc été erigé.

5.7.46 Les procédures pour déconnecter et pour raccorder à nouveau un système hôte au réseau n'étaient pas suffisamment détaillées. Au cours d'une visite sur site, un opérateur qui avait suivi les procédures telles qu'elles étaient rédigées, n'a pas réussi à déconnecter correctement un système hôte. Cela a abouti à une violation des procédures de sécurité du site. Les pratiques ont, par conséquent, été considérées comme défaillantes dans ce domaine et un rapport d'anomalie a été erigé.

5.7.47 La faculté pour tout utilisateur qui utilise la console de terminer des processus dédiés à la sécurité était insuffisamment documentée. Un rapport d'anomalie a été erigé.

5.7.48 La possibilité de rendre inopérants les mécanismes d'imputation pendant l'exécution du système était insuffisamment documentée dans la pratique. Un rapport d'anomalie a été erigé.

5.7.49 Comme les critères de conformité des ITSEC qui concernent le démarrage et l'exploitation n'étaient pas satisfaits, seul un verdict *d'échec* a pu être prononcé. La documentation d'exploitation a ensuite été retravaillée par le commanditaire et par le développeur, puis réexaminée par les évaluateurs. Il a été alors possible de prononcer un verdict *de réussite* selon les critères ITSEC concernant le démarrage et l'exploitation.

5.7.50 Cependant, les évaluateurs ont estimé que le fait de rendre inopérants les mécanismes d'imputation et de terminer depuis la console les processus dédiés à la sécurité pouvait occasionner des **vulnérabilités potentielles**. Ces problèmes ont été notés et examinés par les évaluateurs en tant que partie de leur analyse indépendante des **vulnérabilités**.

Chapitre 5.8 Exemple 7, estimation de l'efficacité (E3)

Introduction

5.8.1 Ce chapitre présente un exemple complètement développé des critères d'efficacité pour E3. Cet exemple est entièrement fictif et de nature théorique. L'exemple ignore l'application des critères de conformité. Il faudrait, par conséquent, supposer que ces critères ont été appliqués au moment approprié.

5.8.2 Les principaux objectifs de cet exemple sont d'illustrer :

a) comment un commanditaire peut fournir de bons arguments pour justifier que les vulnérabilités identifiées ne sont pas exploitables dans la pratique ;

b) le travail effectué par les évaluateurs pour vérifier de façon indépendante l'analyse de vulnérabilité du commanditaire.

5.8.3 Etant donné qu'il s'agit d'un exemple fictif, les vulnérabilités traitées ici ont été simplement choisies pour illustrer l'analyse.

5.8.4 Après que les caractéristiques saillantes de la cible de sécurité et de la conception générale du système pris en exemple aient été décrites, les critères de pertinence et de cohésion de la fonctionnalité sont appliqués. Ces deux critères visent à identifier les vulnérabilités respectivement dans la cible de sécurité et dans la conception générale (voir le chapitre 4.4 de la partie 4). La cible de sécurité utilisée dans l'exemple est telle que l'application du critère de pertinence de la fonctionnalité ne révèle aucune vulnérabilité. Cependant, une conception générale a été choisie pour illustrer un échec (partiel) sur le critère de cohésion de la fonctionnalité.

5.8.5 D'autres exemples de **vulnérabilités en exploitation** et de vulnérabilité de construction sont alors présentés et l'application des estimations de la vulnérabilité en exploitation et de construction, de l'analyse de la résistance des mécanismes et du critère de facilité d'emploi est illustrée. En raison de la simplicité de la cible de sécurité telle que présentée dans cet exemple, les analyses de la résistance des mécanismes et de la facilité d'emploi sont, néanmoins, limitées.

Description de la cible de sécurité

Description du système

5.8.6 Cet exemple de système se trouve sur un site étendu appartenant à une organisation commerciale. Ce site est complètement clôturé par une barrière sur son périmètre et qui est bien surveillée. L'ensemble du personnel est considéré comme étant digne de confiance. Les visiteurs du site sont escortés en permanence.

5.8.7 On trouve sur ce site des zones disposant de protections supplémentaires sous la forme d'un contrôle d'accès physique et de mécanismes organisationnels de sécurité. Les menaces cryptographiques et de type TEMPEST sont faibles. Les terminaux sont situés dans des zones sécurisées et les utilisateurs autorisés empêcheront le personnel d'utiliser un terminal non surveillé qui se trouve dans une pièce qu'il visite.

5.8.8 Sur ce site, on trouve une grande variété de systèmes TI différents, acquis à différentes époques provenant de différents fournisseurs et utilisés pour divers usages tels que la gestion transactionnelle, la facturation ou l'administration de la société.

5.8.9 Chacun de ces systèmes, appelé système d'extrémité, peut être identifié par un numéro de système, S#, et un niveau de sécurité, SL. Ils fournissent chacun le niveau requis de sécurité pour leurs besoins propres (par exemple, certaines informations sont Confidentiel Direction, CD). En raison de la sécurité physique du site, des nombres d'utilisateurs par système d'extrémité, des menaces perçues et de la sensibilité des données, aucun système d'extrémité ne peut garantir plus de protection que celle offerte par un système d'exploitation de la classe F-C2 des critères ITSEC.

5.8.10 Dans le cadre de cet exemple, chaque système d'extrémité, en général, possédera ses propres fonctions d'I&A et de DAC sous le contrôle direct de l'administrateur du système d'extrémité concerné. De plus, tous les systèmes d'extrémité peuvent être considérés comme des réseaux en étoile, comportant un système hôte central (ou grappe) servant une communauté fermée d'utilisateurs utilisant principalement des terminaux "muets".

5.8.11 Les connexions entre les terminaux utilisateurs et les systèmes hôtes, qui peuvent être situés dans des bâtiments différents, ont dans un premier temps été réalisées avec de la fibre optique. Ces connexions sont maintenant remplacées par un SWAN (Site-Wide Area Network). Le SWAN est un réseau TCP/IP en anneau à jeton constitué d'une double boucle contrarotative et de plusieurs sous-anneaux. Un équipement d'un système d'extrémité est raccordé au SWAN par des points d'accès aux hôtes (HAP) ou par des points d'accès aux terminaux (TAP). Les TAP sont desservis par des connexions RS232 à des serveurs de terminaux (TS) et, de là, au moyen d'une connexion Ethernet àdes routeurs principalement raccordés aux sous-anneaux, bien que certains soient connectés directement au fédérateur principal. Les HAP se raccordent directement à un routeur. Ces connexions sont permanentes. Lorsqu'un terminal est mis en route, le SWAN lance automatiquement une séquence de connexion. Si la connexion utilisateur est réussie, un menu comportant les services autorisés est proposé à l'utilisateur sur son terminal. Ce menu affichera la liste des systèmes hôtes auxquels cet utilisateur a accès par autorisation de l'administrateur du SWAN. Un circuit virtuel est alors établi entre ce terminal et le système hôte choisi. L'utilisateur doit alors se connecter au système hôte.

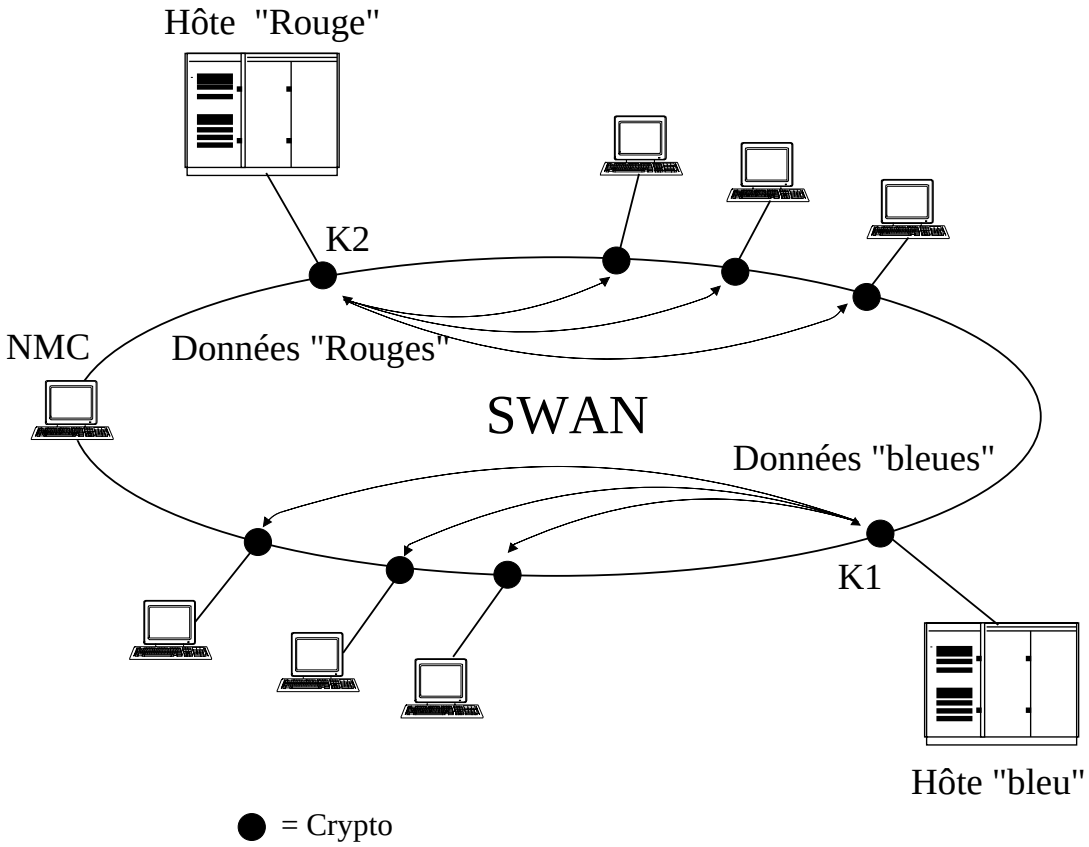
5.8.12 Les profils de sécurité (à quels systèmes hôtes les utilisateurs ont-ils le droit d'accéder ?) et les autres mécanismes de sécurité sont gérés sur le SWAN au moyen d'un ou deux centres de gestion du réseau (NMC), qui fournissent l'I&A, le DAC et le MAC pour le SWAN.

Objectifs de sécurité

5.8.13 Le SWAN fournit donc un service de connexion aux systèmes hôtes du système d'extrémité et à l'ensemble de leurs utilisateurs. Il a deux objectifs de sécurité :

a) empêcher les accès non autorisés à un système d'extrémité (S1) ;

b) assurer la confidentialité des informations en transit (S2).



Le SWAN fournit l'interconnexion entre différents systèmes informatiques et leurs utilisateurs. Le *contrôle d'accès aux systèmes d'extrémité* est fourni par le centre de gestion du réseau (NMC) qui n'accorde l'accès qu'aux services autorisés du réseau. Un utilisateur, du système bleu par exemple, aurait à se connecter au SWAN, puis à choisir un service autorisé et à se connecter alors au système hôte. Plusieurs communautés utilisent le réseau pour gérer des informations de classifications différentes (par exemple, les données rouges peuvent être classifiées Confidentiel Direction et les données bleues non classifiées). Le cloisonnant par communauté est donc nécessaire et obligatoire. *La confidentielle des communications* est assurée par un chiffrement de bout en bout avec des clefs uniques par système d'extrémité (i.e. K1 et K2 dans la figure). Des contrôles physiques et des procédures sont mis en place pour assurer que les utilisateurs n'utilisent que leurs propres terminaux (autrement dit, un utilisateur du système rouge n'est pas autorisé à entrer dans la pièce où se situent les terminaux bleus ni à utiliser l'un de ces terminaux).

Figure 5.8.1 Conception générale du système SWAN

Menaces pour la sécurité

5.8.14 Les menaces envers la sécurité du SWAN sont les suivantes :

a) un utilisateur pourrait se faire passer pour un autre utilisateur (mascarade) lors de l'accès au SWAN (T1) ;

b) un utilisateur pourrait demander ou tenter d'utiliser un service pour lequel il/elle ne possède pas d'autorisation (T2) ;

c) Une personne pourrait écouter ou capturer des données échangées sur le réseau (T3).

d) Un utilisateur pourrait se faire passer pour un autre utilisateur (mascarade) lors de l'accès à un système hôte (T4).

Politique de sécurité

5.8.15 La politique de sécurité spécifie trois formes de contrôle d'accès : le contrôle d'accès obligatoire (MAC), le partage de point d'accès aux hôtes (HAP-sharing) (voir ci-dessous) et le contrôle d'accès discrétionnaire (DAC).

5.8.16 Le MAC est satisfait si et seulement si :

$$S\#_H = S\#_T$$

$$SL_H = SL_T$$

où ($S\#_H$, SL_H) et ($S\#_T$, SL_T) sont respectivement les numéros de système et les niveaux de sécurité du système hôte et du terminal.

5.8.17 La politique de partage de point d'accès aux hôtes (HAP-sharing) rend compte du cas où un terminal peut se voir proposer l'accès à plus d'un système hôte (H1...Hn), et exige :

$$S\#_{H1} = S\#_{H2} = ... \ S\#_{Hn} = S\#_T$$

$$SL_{H1} = SL_{H2} = ... \ SL_{Hn} = SL_T$$

5.8.18 Dans le cadre de ces contraintes, le DAC ne permet que la connexion des éléments d'équipement du système d'extrémité que l'administrateur du système d'extrémité souhaite.

Fonctions de sécurité

5.8.19 La sécurité du SWAN est mise en application par quatre **contre-mesures** (CM1 à CM4) :

a) une fonction d'I&A est utilisée pour authentifier les utilisateurs se connectant au réseau (CM1) ;

b) la politique de contrôle d'accès décrite ci-dessus est mise en application par les centres de gestions du réseau (NMC) (CM2) ;

c) les dispositifs de chiffrement/déchiffrement approuvés sont placés entre les équipements des systèmes d'extrémité et les points d'accès aux hôtes (HAP) et les serveurs de terminaux (ST) (CM3) ;

d) une fonction d'I&A est utilisée pour authentifier les utilisateurs se connectant à un système hôte (CM4).

5.8.20 Les dispositifs cryptographiques qui sont placés entre un système hôte et le SWAN fonctionnent toujours en mode chiffrant - il n'y a pas de contournement en texte clair. Cependant, les dispositifs placés entre un terminal et le réseau possèdent un mode de contournement. Initialement, un dispositif de ce type fonctionne en mode de contournement. Cela permet une interaction en clair avec le réseau (les messages émis vers et depuis le réseau ne sont pas chiffrés). Une fois que l'utilisateur a établi une connexion avec le système hôte, le boîtier de chiffrement du système hôte (HCU) transmet un signal au boîtier de chiffrement du terminal (TCU) qui fait commuter le TCU du mode de contournement en mode chiffré. A l'issue de la session entre l'utilisateur et le système hôte, le circuit est rompu et le TCU revient en mode de contournement. Un voyant sur chaque boîtier de chiffrement est allumé lorsque l'équipement est en mode chiffré et s'éteint lorsque le mode en clair est activé.

5.8.21 Les clefs sont gérées à l'extérieur, c'est-à-dire qu'elles sont sous la responsabilité des administrateurs des systèmes d'extrémité et non de l'administrateur du SWAN. Il y a une clef de chiffrement par système d'extrémité et il n'existe pas deux clefs identiques.

5.8.22 La politique de contrôle d'accès discrétionnaire (DAC) est mise en application par les centres de gestion du réseau (NMC).

5.8.23 Aucun routeur ou logiciel de serveur de terminaux n'est considéré comme touchant à la sécurité.

Résistance minimum des mécanismes exigée

5.8.24 La résistance minimum des mécanismes exigée est *moyenne*. En conséquence (voir l'annexe 6.C en partie 6), les niveaux maxima d'opportunité, de compétence et de ressources d'un attaquant sont considérés comme *moyens.*

5.8.25 Les développeurs choisissent d'utiliser un mécanisme cryptographique coté par l'autorité nationale appropriée comme *moyenne* au moins, un mécanisme de contrôle d'accès (pour CM2) coté *élevée*, et des mécanismes d'I&A *élémentaire* (pour CM1 et CM4).

5.8.26 La cible de sécurité met en avant le fait que le mécanisme cryptographique est un mécanisme critique du SWAN, car si les mécanismes de contrôle d'accès échouent, l'attaquant obtient uniquement l'accès à des données chiffrées, préservant ainsi les deux objectifs de sécurité.

Éléments configurables

5.8.27 Il existe un boîtier de chiffrement élémentaire qui peut être configuré pour être soit un boitier de chiffrement hôte (HCU), soit un boitier de chiffrement terminal (TCU), en insérant une "carte clef" contenant un programme et la clef de chiffrement. Les cartes sont de taille et de couleur différentes et la fente pour introduire les "cartes clef" pour les HCU est obturée mécaniquement de sorte qu'elle ne peut physiquement pas accepter les cartes TCU. Cette fonction distingue réellement les HCU des TCU.

5.8.28 Les mots de passe peuvent être configurés pour être d'une longueur de 8 à 12 caractères et sont générés automatiquement. La durée de vie d'un mot de passe peut être configurée entre 1 et 60 jours. Les deux intervalles sont spécifiés dans la cible de sécurité.

5.8.29 Aucune autre fonction de sécurité n'est configurable.

Analyse de l'efficacité

Analyse de pertinence

5.8.30 Les critères ITSEC exigent du commanditaire qu'il fournisse une **analyse de pertinence**, qui établit un lien entre les fonctions et mécanismes dédiés à la sécurité aux menaces identifiées, que leur conception vise à contrer[1], et qui montrent que ces menaces sont convenablement contrées.

5.8.31 Dans cet exemple, l'analyse de pertinence du commanditaire considère chaque menace énumérée au paragraphe 5.8.14, indépendamment des autres menaces. Cette analyse identifie au moins une fonction ou un mécanisme qui peut contrer cette menace. Le commanditaire ne prend pas en compte la composition des mécanismes, c'est-à-dire que le commanditaire ne considère pas la conception générale du SWAN (figure 5.8.1), mais seulement la simple énumération des menaces et des contre-mesures comme elle est donnée dans la cible de sécurité.

5.8.32 Dans cet exemple, le commanditaire démontre la correspondance directe entre les contre-mesures et les menaces qui concernent les fonctions dédiées à la sécurité comme suit :

a) se faire passer pour quelqu'un d'autre lors d'une tentative d'accès au SWAN (*T1*) et la fonction de connexion au SWAN (*CM1*) ;

b) demander ou obtenir l'accès à un service non autorisé (*T2*) et la fonction de contrôle d'accès au SWAN (*CM2*) ;

c) écouter ou capturer les données en transit sur le SWAN (*T3*) et la fonction de chiffrement (*CM3*) ;

d) se faire passer pour quelqu'un d'autre lors d'une tentative afin d'obtenir un accès à un système hôte (*T4*) et la fonction de connexion à un système hôte (*CM4).*

5.8.33 L'analyse de pertinence du commanditaire inclut le tableau présenté en figure 5.8.2, qui démontre la correspondance entre les objectifs de sécurité, les contre-mesures et les menaces.

1. NdT : ITSEC 3.14.La traduction a été reprise.

Figure 5.8.2 Analyse de pertinence		
Objectifs de sécurité	**Contre-mesures**	**Menaces**
S1 - Accès protégé au système hôte	CM1 - Connexion au SWAN	T1 - mascarade pour l'accès au SWAN
S1 - Accès protégé au système hôte	CM2 - Contrôle d'accès à l'hôte	T2 - demande ou obtention de l'accès à un service non autorisé
S1 - Accès protégé au système hôte	CM4 - Connexion à l'hôte	T4 - mascarade envers le système hôte
S2 - Confidentialité du réseau	CM3 - chiffrement	T3 - capture de données

5.8.34 Les fonctions de connexion, tant celles du SWAN que celles des systèmes hôtes, sont des systèmes spécifiques à mot de passe secret. Dans l'analyse de pertinence du commanditaire, il est soutenu que ces deux fonctions sont pertinentes, dans la mesure où il faudrait qu'un attaquant connaisse le mot de passe secret de l'autre personne pour réussir. Il est également soutenu que :

a) la fonction de contrôle d'accès au SWAN est pertinente car elle n'autorisera un utilisateur identifié qu'à choisir les services pour lequels cette personne a l'autorisation ;

b) la fonction de chiffrement est pertinente car le boîtier de chiffrement du système hôte ne possède pas de mode de contournement et transmet toujours les données chiffrées avec un algorithme approprié et une clef unique à cette machine, connue seulement des utilisateurs autorisés de cet hôte.

5.8.35 Par conséquent, seul un utilisateur *autorisé* qui écouterait ou capturerait les données en transit sur le SWAN serait capable de déchiffrer les données. En conclusion, toutes les fonctions dédiées à la sécurité sont donc pertinentes.

5.8.36 Il faut remarquer que ces arguments ne se soucient pas de la résistance des mécanismes ou de la cohésion des fonctions de sécurité.

5.8.37 Un exemple de fonction non pertinente serait l'utilisation d'une fonction de DAC pour empêcher quelqu'un, n'ayant pas l'habilitation requise, d'accéder à des informations classifiées. En effet, une fonction de DAC n'est pas en mesure de déterminer les classifications des objets et les habilitations des sujets avec lesquels elle opère.

5.8.38 Alternativement, l'argument pour la pertinence aurait pu être reformulé en termes d'objectifs de sécurité. Cette approche peut être préférable dans le cas d'un produit ou lorsque la menace est exprimée de façon plus grossière, par exemple "il existe une menace terroriste" :

a) L'objectif portant sur l'accès à un système d'extrémité (S1) est satisfait par la combinaison des fonctions de connexion (CM1 et CM4) et de la fonction de contrôle d'accès (CM2) (pour les raisons données dans le paragraphe 5.8.34).

b) La confidentialité des informations en transit (S2) est protégée par le mécanisme cryptographique (CM3) (pour les raisons données dans le paragraphe 5.8.34).

Analyse de cohésion

5.8.39 Les critères ITSEC[1] exigent du commanditaire :

a) qu'il fournisse une analyse de toutes les relations potentielles entre les fonctions et mécanismes dédiés à la sécurité ;

b) qu'il montre qu'il est impossible d'amener l'une des fonctions ou l'un des mécanismes dédiés à la sécurité à rentrer en conflit ou à se mettre en contradiction avec d'autres fonctions ou mécanismes dédiés à la sécurité.

5.8.40 A la différence de la pertinence de la fonctionnalité, l'**analyse de cohésion** doit prendre en compte la composition du système, c'est-à-dire que le développeur doit considérer *toutes les relations potentielles entre les fonctions et mécanismes dédiés à la sécurité*.

5.8.41 Dans cet exemple, le contrôle d'accès du système d'extrémité est violé si des données ROUGES peuvent être affichées sur un terminal BLEU. La confidentialité des communications est violée si les clefs de chiffrement sont compromises, si les boîtiers de chiffrement du terminal ou des hôtes sont contournés tous les deux et la transmission s'effectue "en clair", ou si tout autre information "utile" est transmise en clair.

5.8.42 L'analyse de cohésion du commanditaire montre que :

a) si l'utilisateur (attaquant) échoue dans sa tentative de connexion au SWAN, pour quelque raison que ce soit, aucune information utile ne peut être obtenue ;

b) si l'utilisateur se connecte au SWAN avec succès, les dispositifs cryptographiques placés entre le terminal et le SWAN fonctionnent en mode de contournement jusqu'à ce qu'une connexion soit établie avec un système hôte. Par conséquent, les données d'authentification du SWAN seront transmises en clair sur le SWAN ;

c) l'utilisateur ne se voit offrir que des services (i) auxquels il a droit et (ii) qui satisfont à la politique de contrôle d'accès du SWAN ;

d) une liaison chiffrée est alors établie entre le terminal et le système hôte. Le développeur suppose que seules des clefs adéquates sont utilisées ;

e) l'utilisateur se connecte alors au système hôte. S'il échoue, le processus s'arrête : aucune donnée utile n'aura été affichée sur le terminal et aucune autre donnée utile n'aura été transmise sur le SWAN (autre que les données d'authentification du SWAN, voir (b) ci-dessus) ;

1. NdT : ITSEC 3.18 et 3.19.La traduction a été reprise.

f) si l'utilisateur réussit, il peut alors transférer des informations *chiffrées* entre son terminal et le système hôte.

5.8.43 L'analyse de cohésion du commanditaire présente trois scénarios (voir figure 5.8.3).

Figure 5.8.3 Analyse de cohésion

Scénario	**Données affichées**	**Données sur le SWAN**
L'utilisateur échoue dans sa connexion au SWAN	Aucune	Aucune
L'utilisateur se connecte au SWAN mais échoue dans sa connexion à l'hôte	Aucune	Information d'I&A *en clair*
L'utilisateur se connecte au SWAN et à un service *autorisé* de l'hôte	Données BLEUES	Information d'I&A *en clair* Données chiffrées

5.8.44 Par conséquent, le commanditaire est en mesure de montrer que :

a) les fonctions d'I&A du SWAN, de contrôle d'accès et d'I&A de l'hôte *sont cohésives*, car pour chacun des scénarios, des données ROUGES ne sont jamais affichées en clair ;

b) les dispositifs de chiffrement, cependant, *ne sont pas entièrement cohésifs entre-eux*, car pour certains scénarios, des données d'authentification du SWAN sont transmises en clair.

5.8.45 Le commanditaire soutient alors que la mise en échec de CM1 n'est pas suffisante en soi pour violer les objectifs de sécurité car, bien que les données d'authentification du SWAN soient transmises "en clair", les mécanismes cryptographiques (CM3) et la connexion à l'hôte (CM4) assurent encore l'application de la politique de sécurité.

5.8.46 Les évaluateurs effectuent une vérification indépendante de l'analyse de cohésion du commanditaire. Le manque apparent de cohésion est noté, mais les évaluateurs ne prononcent pas un verdict *d'échec* à ce point de l'estimation de l'efficacité.

5.8.47 Ce manque de cohésion présente simplement une vulnérabilité que les évaluateurs doivent vérifier indépendamment pour déterminer si elle est exploitable dans la pratique. A ce stade, il n'est pas possible de prononcer un verdict *d'échec*, sauf s'il peut être montré que cette vulnérabilité (de construction) est exploitable. Ceci ne peut être déterminé qu'après que les évaluateurs aient appliqué les critères d'estimation de la vulnérabilité et aient effectué les tests de pénétration.

Analyses de vulnérabilité du commanditaire

5.8.48 Conformément aux critères ITSEC (paragraphes 3.26 à 3.27 et 3.35 à 3.36), le commanditaire fournit aux évaluateurs une liste des vulnérabilités connues dans la construction et l'exploitation de la cible d'évaluation, ainsi qu'une analyse des impacts potentiels de chaque vulnérabilité connue sur la sécurité de la cible d'évaluation.

5.8.49 Dans cet exemple, le commanditaire a combiné la liste des vulnérabilités de construction connues et la liste des vulnérabilités en exploitation connues et a effectué une seule analyse de vulnérabilité.

5.8.50 Les vulnérabilités en exploitation sont associées aux procédures physiques et administratives externes à la cible d'évaluation. Elles peuvent fournir à un attaquant l'occasion et les ressources nécessaires pour exploiter une **vulnérabilité de construction** ou pour perpétrer une attaque directe. Elles peuvent également fournir à l'attaquant l'information de sécurité (par exemple, l'identifiant et le mot de passe d'un utilisateur) nécessaire pour se faire passer pour un utilisateur autorisé.

5.8.51 Les critères ITSEC exigent du commanditaire qu'il montre que la vulnérabilité n'est pas réellement exploitable en pratique, ce qui signifie que :

a) chaque vulnérabilité est convenablement couverte par d'autres mécanismes de sécurité non compromis, ou ;

b) la vulnérabilité ne relève pas de la cible de sécurité, n'existera pas dans la pratique ou est contrée par des contre-mesures techniques, liées au personnel, organisationnelles ou physiques extérieures à la cible d'évaluation.

5.8.52 Les vulnérabilités de construction et en exploitation identifiées par le commanditaire sont présentées en figure 5.8.4. Cette liste rapproche les vulnérabilités des menaces (par exemple, l'écoute clandestine des données d'I&A du SWAN pourrait permettre à un utilisateur de se faire passer pour un autre utilisateur lors de l'accès au SWAN, menace T1) et de l'objectif de sécurité qui peut être violé si la vulnérabilité est réellement exploitable en pratique.

5.8.53 Pour obtenir un accès aux données d'un système hôte en violant la politique de sécurité, un attaquant doit exécuter avec succès un *scénario d'attaque* traversant les quatre contre-mesures (CM1 à CM4). Chaque contre-mesure rencontrée au cours du scénario d'attaque doit être franchie soit par une attaque directe (par exemple, une attaque portant sur les algorithmes sous-jacents, les principes ou propriétés de la contre-mesure concernée), soit de façon indirecte (par exemple, le contournement).

5.8.54 La figure 5.8.5 montre l'analyse du commanditaire de tous les scénarios d'attaque possibles qui violeraient les objectifs de sécurité, pour :

a) protéger contre les accès non-autorisés à un système d'extrémité (S1) ;

b) protéger la confidentialité des informations en transit (S2).

5.8.55 Les moyens pour mettre en échec[1] les contre-mesures CM1 à CM4 comprennent la manifestation des menaces correspondantes T1 à T4, qui peut être réalisée par attaque indirecte de ces contre-mesures en exploitant les vulnérabilités précédemment identifiées (par exemple, V1 et V2 sont des attaques indirectes de CM1).

5.8.56 Si un attaquant dispose d'un compte licite sur le système hôte, alors l'attaquant a le choix entre utiliser normalement le menu des services autorisés du SWAN ou invoquer V6. Si l'attaquant ne dispose pas d'un compte licite sur le système hôte, alors l'attaquant ne peut qu'utiliser V6 car si l'hôte ciblé figurait au menu des services autorisés, l'utilisateur aurait normalement un compte licite sur cet hôte. V6 requiert la collusion avec l'administrateur de la sécurité du SWAN, mais pas celle de l'administrateur de la sécurité de l'hôte ciblé, d'où le besoin d'attaquer la connexion hôte.

5.8.57 Même s'il est dans l'intention du développeur que les contre-mesures dussent être franchies dans l'ordre CM1, CM2, CM3 et CM4, il est possible, étant donné la construction du SWAN, que d'autres scénarios d'attaque qui conduisent à une **vulnérabilité exploitable** puissent exister.

5.8.58 Dans cet exemple, l'analyse du commanditaire ne montre aucun moyen permettant de contourner le mécanisme cryptographique, la seule vulnérabilité identifiée étant une désactivation par un complice. Par conséquent, pour chaque scénario d'attaque de la figure 5.8.5, l'attaquant doit mettre en échec la contre-mesure CM3 pour violer les objectifs de sécurité S1 et S2.

5.8.59 La contre-mesure CM3 a une RdM à une attaque directe cotée *moyenne* et atteint la RdM minimum annoncée pour le SWAN. Un attaquant pourrait tenter de profiter de la vulnérabilité de construction V4, mais ceci nécessite de toute évidence la collusion d'un utilisateur réel de l'hôte ciblé et est traité par des mesures de sécurité extérieures à la cible d'évaluation.

5.8.60 L'analyse du commanditaire montre, par conséquent, dans la figure 5.8.5 que les vulnérabilités identifiées sont convenablement contrées par les dispositifs cryptographiques (et les mesures extérieures à la cible d'évaluation).

5.8.61 Comme il n'existe aucun moyen apparent, à part ceux énumérés ci-dessus, de contourner une quelconque contre-mesure dans le scénario d'attaque, il est clair que l'analyse du commanditaire a pris en compte toutes les combinaisons de vulnérabilités identifiées. De la même manière, d'après leur connaissance de la cible d'évaluation, les évaluateurs sont convaincus que l'analyse du commanditaire ne comporte aucune hypothèse déraisonnable quant à l'environnement prévu.

1. NdT : ITSEC 3.8:1. La traduction a été reprise.

Figure 5.8.4 Liste des vulnérabilités connues de construction et en exploitation

ID	Description	Menaces	Objectifs de sécurité
V1	**L'attaquant écoute des données d'I&A sur le SWAN.** Par écoute sur le réseau SWAN, l'attaquant obtient l'identifiant et le mot de passe d'un utilisateur du système hôte ciblé (l'hôte attaqué). Cette vulnérabilité a été identifiée grâce à l'analyse de cohésion précédente.	T1	S1
V2	**Touche "break" pendant la connexion au SWAN.** Une frappe de la touche "break" au moment de la connexion au SWAN provoque l'expiration du processus de connexion au bout de 5 minutes, à condition que l'utilisateur ne tape rien. Un message d'expiration du processus est affiché. À condition que l'utilisateur ne fasse rien pendant 10 minutes, le message arrive lui-même à expiration alors que le menu des services autorisés pour le dernier utilisateur qui s'est connecté avec succès est affiché. Cet utilisateur pourrait être un utilisateur de l'hôte attaqué.	T1	S1
V3	**Services non autorisés accessibles.** Si le nombre de services autorisés pour l'utilisateur courant est moins élevé que pour l'utilisateur précédent, les services supplémentaires (non autorisés) sont toujours accessibles bien qu'ils ne soient pas affichés.	T2	S1
V4	**Un complice désactive le chiffrement.** Une double frappe rapide de la touche "break" au moment de la connexion à l'hôte provoque que le TCU contourne le chiffrement sans que le NMC ne reçoive la consigne de couper la session avec l'hôte. Une frappe supplémentaire de la touche "break" le fait, mais, à cause d'un défaut de le HCU, toutes les transmissions ultérieures entre le HCU et n'importe quel TCU sont en clair. Comme la connexion à l'hôte est protégée par le HCU, la désactivation de ce HCU n'est possible que par un utilisateur autorisé de cet hôte, d'où la nécessité d'un complice.	T3	S2
V5	**Un complice a capturé des données d'I&A d'une machine hôte .** L'utilisation d'une séquence particulière de touches de fonction permet à un utilisateur d'obtenir l'accès à la table des mots de passe du système hôte. Les mots de passe sont chiffrés mais peuvent être décryptés en quelques jours. Cela ne peut être réalisé que par un utilisateur réel du système hôte comme pour V4 ci-dessus.	T4	S1
V6	**Un attaquant a été autorisé à un service par collusion.** Les services autorisés sont accordés à un utilisateur sur présentation d'une demande écrite de l'utilisateur et acceptée par son supérieur hiérarchique. Cette information est contrôlée par comparaison avec d'autres utilisateurs et est rejetée par le NMC si elle ne respecte pas la politique de contrôle d'accès au SWAN. L'information est saisie sous le contrôle de deux personnes. Même avec ces précautions, il est possible, par collusion, d'utiliser le même numéro de système, *S#*, et le même niveau de sécurité, *SL*, que ceux de l'hôte attaqué pour identifier un nouveau système et d'utiliser le DAC pour séparer les deux communautés d'utilisateurs des deux systèmes, mais en accordant à l'attaquant l'accès aux deux.	T2	S1

Figure 5.8.5 Analyse par le commanditaire des scénarios d'attaque

Séq	Description	CM1 (élémentaire)	CM2 (élevée)	CM3 (moyenne)	CM4 (élémentaire)	Viole
1	L'attaquant met en échec CM1, se sert du menu d'autorisation SWAN normalement, met en échec CM3 et se connecte avec succès à l'hôte	V1 ou V2	utiliser le menu	V4	se connecter à l'hôte en tant qu'utilisateur autorisé	S1,S2
2	L'attaquant met en échec CM1, se sert du menu d'autorisation SWAN normalement puis met en échec CM3 et CM4	V1 ou V2	utiliser le menu	V4	V5	S1,S2
3	L'attaquant met en échec CM1 à CM4 en utilisant une combinaison des vulnérabilités précédentes	V1 ou V2	V6 ou V3	V4	V5	S1,S2
4	L'attaquant met en échec CM1 à CM3 et réalise alors avec succès une connexion à l'hôte	V1 ou V2	V3	V4	se connecter à l'hôte en tant qu'utilisateur autorisé	S1,S2
5	L'attaquant se connecte avec succès au SWAN puis met en échec CM2 à CM4	se connecter au SWAN en tant qu'utilisateur autorisé	V6 ou V3	V4	V5	S1,S2
6	L'attaquant se connecte avec succès au SWAN, met en échec CM2 et CM3, puis se connecte avec succès à l'hôte	se connecter au SWAN en tant qu'utilisateur autorisé	V3	V4	se connecter à l'hôte en tant qu'utilisateur autorisé	S1,S2
7	L'attaquant se connecte avec succès au SWAN, choisit un service autorisé puis met en échec CM3 et CM4	se connecter au SWAN en tant qu'utilisateur autorisé	sélectionner un service autorisé	V4	V5	S1,S2
8	L'attaquant se connecte avec succès au SWAN, choisit un service autorisé, met en échec CM3 puis se connecte avec succès à l'hôte	se connecter au SWAN en tant qu'utilisateur autorisé	sélectionner un service autorisé	V4	se connecter à l'hôte en tant qu'utilisateur autorisé	S2

Analyse indépendante de vulnérabilité des évaluateurs

5.8.62 Les critères ITSEC[1] exigent des évaluateurs qu'ils effectuent une analyse indépendante de vulnérabilité en prenant en compte les vulnérabilités énumérées et toutes les autres vulnérabilités connues (vulnérabilités en exploitation comme de construction) découvertes au cours de l'évaluation.

5.8.63 Tout au long de cet exemple, on a supposé que les critères de conformité avaient déjà été appliqués à la cible d'évaluation. Pour l'exemple, il est supposé que l'application des critères de conformité a identifié une vulnérabilité potentielle qui, après analyse, a été considérée comme une vulnérabilité de construction. Cette vulnérabilité n'était pas encore identifiée dans la liste des vulnérabilités connues du commanditaire. Cette vulnérabilité est identifiée dans la figure 5.8.6.

Figure 5.8.6 Vulnérabilités de construction découvertes au cours de l'estimation de la conformité

ID	Description	Menace	Objectifs de sécurité
V7	**L'utilisateur désactive les boitiers de chiffrement** La vulnérabilité est la même que V4, mais si l'attaquant est un utilisateur autorisé, il est son propre complice. Cette situation peut se produire par exemple si l'attaquant est un utilisateur d'un système à données Confidentiel Direction disposant d'un accès autorisé seulement à partir d'un terminal situé dans un local habilité mais l'attaquant souhaite accéder au système à partir de son bureau (non habilité).	T3	S2

5.8.64 La conséquence de cette vulnérabilité de construction est qu'un utilisateur qui s'est connecté avec succès à un système hôte ROUGE a la faculté de mettre en échec la contre-mesure CM3 sans besoin de collusion. Cette vulnérabilité affecte les scénarios d'attaque 1, 4, 6 et 8 dans l'analyse de l'évaluateur des séquences d'attaque, qui sont désormais les scénarios indiqués en figure 5.8.7. Les évaluateurs s'inquiétaient que l'analyse de vulnérabilité du commanditaire ait montré que :

a) CM1 et CM4 sont cotées avec une RdM *élémentaire* et, séparément, ne sont pas adéquates (à noter que seuls les mécanismes pour CM2 (*élevée*) et CM3 (*moyenne*) atteignent la RdM minimum annoncée pour la cible d'évaluation (*moyenne*)) ;

b) le mécanisme pour CM3 est le seul dans les scénarios d'attaque 1, 2, 7 et 8 qui atteigne la RdM minimum annoncée pour le SWAN (le scénario d'attaque 8 repose entièrement sur CM3 pour maintenir la politique de sécurité) ;

c) si le mécanisme pour CM2 peut être mis en échec, alors le mécanisme pour CM3 est le seul dans les scénarios d'attaque 3, 4, 5 et 6 qui atteigne la RdM minimum annoncée pour le SWAN.

1. NdT : ITSEC 3.25 à 3.28 et 3.34 à 3.37.La traduction a été reprise.

Figure 5.8.7 Analyse par les évaluateurs des scénarios d'attaque

Séq	Description	CM1 (élémentaire)	CM2 (élevée)	CM3 (moyenne)	CM4 (élémentaire)	Viole
1'	L'attaquant brise CM1, se sert du menu d'autorisation SWAN normalement, brise CM3 et se connecte avec succès à l'hôte	V1 ou V2	selectionner un service autorisé	V4 ou V7	se connecter à l'hôte en tant qu'utilisateur autorisé	S1,S2
4'	L'attaquant brise CM1à CM3 et réalise alors avec succès une connexion à l'hôte	V1 ou V2	V3	V4 ou V7	se connecter à l'hôte en tant qu'utilisateur autorisé	S1,S2
6'	L'attaquant se connecte avec succès au SWAN, brise CM2 et CM3, puis se connecte avec succès à l'hôte	se connecter au SWAN en tant qu'utilisateur autorisé	V3	V4 ou V7	se connecter à l'hôte en tant qu'utilisateur autorisé	S1,S2
8'	L'attaquant se connecte avec succès au SWAN, choisit un service autorisé, brise CM3 puis se connecte avec succès à l'hôte	se connecter au SWAN en tant qu'utilisateur autorisé	selectionner un service autorisé	V4 ou V7	se connecter à l'hôte en tant qu'utilisateur autorisé	S2

5.8.65 Il n'est pas possible de prononcer un verdict final sur les estimations de vulnérabilité (voir la section *Verdicts de l'évaluateur*, chapitre 4.4, partie 4) avant que les évaluateurs ne soient en mesure de prouver si oui ou non cette nouvelle vulnérabilité de construction (ou n'importe laquelle des vulnérabilités précédentes) est réellement exploitable en pratique (par des tests de pénétration).

Résistance des mécanismes

5.8.66 Bien que le commanditaire ait coté tous les mécanismes (voir le paragraphe 5.8.25), l'analyse de vulnérabilité du commanditaire montre que le seul mécanisme critique est celui de CM3 (ceci a également été confirmé par l'analyse indépendante de vulnérabilité des évaluateurs).

5.8.67 La contre-mesure CM3 est cryptographique et l'estimation de la résistance de son mécanisme cryptographique est hors du champ des critères ITSEC, de même que les procédures de gestion de clefs. Les évaluateurs peuvent uniquement vérifier, par référence à l'autorité nationale compétente, que le mécanisme cryptographique atteint la cotation de la résistance minimum des mécanismes annoncée pour le SWAN.

5.8.68 Les évaluateurs doivent demander à l'autorité nationale compétente si la RdM des boîtiers de chiffrement, y compris les procédures de gestion de clefs, serait cotée au moins *moyenne*, autant dans le contexte d'une analyse cryptographique en ligne (demandée pour une attaque du cloisonnement des systèmes d'extrémité, en raison du besoin d'établir une voie de communication avec le système hôte) que dans le contexte d'une analyse cryptographique hors ligne (pour l'écoute).

5.8.69 Pour l'exemple, il est affirmé que la réponse aux deux questions est positive et, vu que le mécanisme critique est un boîtier de chiffrement, aucun test de pénétration concernant une attaque directe ou une vulnérabilité en exploitation n'est entrepris par les évaluateurs. En conséquence, les évaluateurs sont en mesure de prononcer un verdict *de réussite* par rapport au critère de résistance des mécanismes.

5.8.70 Dans cet exemple, il n'y a qu'un seul mécanisme critique, commun aux deux objectifs de sécurité. Dans d'autres cas, lorsqu'il existe de multiples objectifs de sécurité, les mécanismes critiques pour chaque objectif peuvent être différents.

5.8.71 En outre, une attaque cryptographique en ligne est très difficile à réaliser, sinon impossible, sans contourner les procédures de gestion de clefs afin que des "mauvaises" clefs soient utilisées. Dans une attaque hors ligne, comme dans le cas du scénario d'attaque 8', il peut être possible de déduire la clef d'après l'analyse du texte chiffré. Dans cet exemple, la RdM de l'algorithme et les procédures de gestion de clefs sont suffisamment "fortes" pour empêcher que cela ne se produise.

5.8.72 L'analyse de la résistance des mécanismes du commanditaire fournit une justification détaillée décrivant le mécanisme de contrôle d'accès du SWAN (CM2) comme un mécanisme "dur", i.e. un mécanisme qui ne peut faire l'objet d'une attaque directe (voir l'annexe 6.C en partie 6). Ceci se traduit dans l'analyse du commanditaire par l'attribution d'une résistance *élevée* à ce mécanisme.

Facilité d'emploi

5.8.73 Cet aspect de l'efficacité examine[1] si la cible d'évaluation peut être configurée ou utilisée d'une manière qui n'est pas sûre, mais qu'un administrateur ou un utilisateur final de la cible d'évaluation pourrait raisonnablement croire sûre.

5.8.74 L'analyse de la facilité d'emploi du commanditaire doit identifier les modes possibles d'exploitation de la cible d'évaluation, y compris l'exploitation à la suite d'une panne ou d'une erreur d'exploitation, leurs conséquences et leurs implications sur le maintien de l'exploitation sûre. Elle doit également montrer :

a) que toute erreur humaine ou autre dans l'exploitation, qui désactive ou rend inopérante des fonctions ou des mécanismes dédiés à la sécurité, sera facilement détectable ;

b) que dans le cas où il est possible de configurer la cible d'évaluation ou de faire en sorte qu'elle puisse être exploitée de façon non sûre (i.e. les fonctions et les mécanismes dédiés à la sécurité de la cible d'évaluation ne satisfont pas à la cible de sécurité), alors qu'un utilisateur final ou un administrateur pourraient raisonnablement la croire sûre, alors cet état de fait sera également facile à détecter.

1. NdT : ITSEC 3.30 à 3.31. La traduction a été reprise.

5.8.75 Les états non sûrs connus de la cible d'évaluation sont identifiés par les scénarios d'attaque. Leur existence même indique qu'il *est* possible d'utiliser ou de configurer la cible d'évaluation de façon non sûre (*un attaquant a l'autorisation pour un service par collusion* est un problème de configuration). La question est donc de savoir si dans un cas pareil, un administrateur ou un utilisateur final pourraient raisonnablement croire que la cible d'évaluation est sûre.

5.8.76 Le commanditaire affirme que le comportement de la cible d'évaluation à la suite d'une panne ou d'une erreur d'exploitation, y compris leurs conséquences et leurs implications sur le maintien de l'exploitation sûre, a déjà été considéré - sinon la liste des vulnérabilités fournie par le commanditaire serait incomplète. Autrement dit, si de nouvelles vulnérabilités étaient introduites (par exemple, une panne électrique des boîtiers de chiffrement), à ce stade, il serait nécessaire de reconsidérer les critères d'estimation de vulnérabilité.

5.8.77 Etant donné les analyses précédentes dans cet exemple, ce critère aborde simplement la possibilité de détecter si les mécanismes critiques de la cible d'évaluation ont échoué. Si un mécanisme critique échoue, alors la cible d'évaluation se trouve dans un état non sûr, ou risque de l'être. Le critère des ITSEC exige simplement que la cible d'évaluation détecte ce fait.

5.8.78 Le commanditaire consate que chaque boîtier de chiffrement possède un voyant qui est allumé lorsque cet équipement fonctionne en mode chiffrant et qui s'éteint lorsqu'il le fait en mode clair. Les évaluateurs savent que ces boîtiers fonctionnent correctement (pour l'exemple, on suppose que les critères de conformité ont été appliqués avec succès). Les voyants de tous les HCU des systèmes hôtes actifs devraient être allumées en permanence, indiquant clairement que le cloisonnement des systèmes d'extrémité et la confidentialité des communications sont respectés.

5.8.79 On constatera cependant que cette analyse peut devenir plus complexe si d'autres fonctions sont présentes dans la cible de sécurité (par exemple, des fonctions d'imputabilité).

Tests de pénétration

5.8.80 A ce point de l'évaluation du SWAN, les évaluateurs ont achevé l'ensemble des activités de conformité et ont prononcé un verdict final *de réussite* sur la conformité de l'ensemble du SWAN. Cependant, suite à l'identification d'une vulnérabilité potentielle au cours de l'estimation de la conformité, les évaluateurs ont mis en évidence une vulnérabilité de construction qui n'avait pas été identifiée par le commanditaire et qui n'avait donc pas été prise en compte dans l'analyse de vulnérabilité du commanditaire.

5.8.81 Ainsi qu'il a été dit au chapitre 4.4 de la partie 4, les évaluateurs ne sont pas en mesure de prononcer un verdict final sur l'efficacité avant que les tests de pénétration n'aient été achevés. L'objectif des tests de pénétration (tel que défini par les ITSEC) est de confirmer ou d'infirmer que les vulnérabilités connues dans la construction ou pour l'exploitation du SWAN sont réellement exploitables en pratique.

5.8.82 Dans cet exemple, les tests de pénétration du SWAN réalisés par les évaluateurs confirment que si un attaquant est l'utilisateur d'un système hôte, alors l'attaquant peut désactiver les dispositifs de chiffrement (V7) sans qu'ils aient besoin d'outils ou de connaissances spécialisés (les évaluateurs y sont parvenus sans aucune aide et en quelques minutes). En revenant à l'analyse indépendante de vulnérabilité des évaluateurs, la figure 5.8.7 indique que les scénarios d'attaque 1', 4', 6' et 8' sont tous affectés par cette vulnérabilité.

5.8.83 Le mécanisme cryptographique est le seul mécanisme critique du SWAN. Dans les scénarios d'attaque 1' et 8', si le mécanisme cryptographique échoue, alors l'objectif de sécurité S2 est immédiatement compromis et l'objectif de sécurité S1 n'est alors défendu que par des mécanismes *élémentaire*s qui n'atteignent pas la cotation annoncée de la résistance minimum des mécanismes du SWAN (*moyenne*).

5.8.84 Par ailleurs, les scénarios d'attaque 4' et 6' exigent également de l'attaquant qu'il mette en échec CM2 (cotée *élevée*) pour violer l'objectif de sécurité S2, mais les résultats des tests de pénétration du SWAN réalisés par les évaluateurs montrent que CM2 pourrait être mise en échc par un attaquant ne bénéficiant d'aucune aide et en quelques jours (du fait de la vulnérabilité de construction V3).

5.8.85 Par conséquent, la vulnérabilité V7 est réellement exploitable en pratique et les évaluateurs prononcent un verdict *d'échec* sur l'analyse de vulnérabilité de la construction, et donc, un verdict final *d'échec* est prononcé sur l'efficacité de la cible d'évaluation.

Chapitre 5.9 Exemple 8, examiner la sécurité des développeurs (E2 et E4)

Introduction

5.9.1 Cet exemple présente deux sous-exemples (8(a) et 8(b)), chacun d'eux aborde un aspect de l'environnement de développement à différents niveaux d'évaluation.

Exemple 8(a) - Examiner la sécurité des développeurs (E2)

Introduction

5.9.2 Ce sous-exemple traite des tâches de l'évaluateur de "L'environnement de développement, aspect 3 - Sécurité des développeurs". L'objectif premier de cet exemple est d'illustrer comment la sécurité du développeur peut être examinée. Des mesures de sécurité physiques et organisationnelles ont été utilisées pour protéger l'environnement de développement.

Exigences des critères ITSEC concernant le contenu et la présentation

5.9.3 *E2.21 Le document portant sur la sécurité de l'environnement de développement doit présenter les protections prévues pour assurer l'intégrité de la TOE et la confidentialité des documents associés. Des mesures de sécurité physiques, organisationnelles, liées au personnel ou autres, utilisées par le développeur, doivent être présentées.*

Exigences des critères ITSEC concernant les éléments de preuve

5.9.4 *E2.22 Les informations concernant la sécurité de l'environnement de développement doivent présenter la manière dont l'intégrité de la TOE et la confidentialité de la documentation associée sont maintenues.*

Tâches de l'évaluateur consignées dans les critères ITSEC

5.9.5 *E2.23 Vérifier que les procédures documentées sont appliquées. Vérifier que les informations fournies sont conformes aux exigences concernant le contenu, la présentation et les éléments de preuve. Rechercher des erreurs dans les procédures.*

Fournitures d'évaluation concernées

5.9.6 Les données pour ce travail sont les informations sur la sécurité de l'environnement de développement fournie par le commanditaire et la cible de sécurité du produit ou système comportant les menaces réelles ou supposées .

Travail effectué

5.9.7 L'information sur les mesures de sécurité était *présentée* dans la documentation du développeur concernant la sécurité. La documentation a été examinée par les évaluateurs (en la lisant et la comprenant). Les évaluateurs ont notamment vérifié que :

a) les mesures de sécurité physiques étaient appropriées pour protéger l'environnement de développement contre une attaque délibérée ;

b) les mesures de sécurité organisationnelles étaient adéquates pour protéger l'intégrité de la cible d'évaluation et pour maintenir la confidentialité de la documentation associée.

5.9.8 Les évaluateurs ont pu visiter le site de développement et confirmer que les mesures de sécurité présentées par le commanditaire étaient appliquées, par :

a) une estimation de la conformité d'autres documentations fournies par rapport aux procédures des mesures de sécurité ;

b) un entretien avec les membres de l'équipe de développement pour vérifier s'ils étaient au courant des procédures et s'ils les appliquaient dans la pratique.

5.9.9 Afin de vérifier plus avant que les procédures documentées étaient appliquées, les évaluateurs ont alors :

a) vérifié l'application des mesures de sécurité physiques ;

b) vérifié l'application des mesures de sécurité organisationnelles.

Exemple 8(b) - Examiner la sécurité des développeurs (E4)

Introduction

5.9.10 Ce sous-exemple traite des tâches de l'évaluateur de "L'environnement de développement, aspect 3 - Sécurité des développeurs". L'objectif premier de cet exemple est d'illustrer comment la sécurité des développeurs peut être examinée. Des mesures de sécurité physiques, organisationnelles et techniques ont été utilisées pour protéger l'environnement de développement.

Exigences des critères ITSEC concernant le contenu et la présentation

5.9.11 *E4.21 Le document portant sur la sécurité de l'environnement de développement doit décrire les protections prévues pour assurer l'intégrité de la TOE et la confidentialité des documents associés. Des mesures de sécurité physiques, organisationnelles, liées au personnel ou autres, utilisées par le développeur, doivent être décrites.*

Exigences des critères ITSEC concernant les éléments de preuve

5.9.12 *E4.22 Les informations concernant la sécurité de l'environnement de développement doivent décrire la manière dont l'intégrité de la TOE et la confidentialité de la documentation associée sont maintenues.*

Tâches de l'évaluateur consignées dans les critères ITSEC

5.9.13 *E4.23 Vérifier que les procédures documentées sont appliquées. Vérifier que les informations fournies sont conformes aux exigences concernant le contenu, la présentation et les éléments de preuve. Rechercher des erreurs dans les procédures.*

Fournitures d'évaluation concernées

5.9.14 Les données pour ce travail sont les informations sur la sécurité de l'environnement de développement fournie par le commanditaire et la cible de sécurité du produit ou du système pour contenir les menaces réelles ou supposées.

Travail effectué

5.9.15 L'information sur les mesures de sécurité était *décrite* dans la documentation du développeur concernant la sécurité. La documentation a été examinée par les évaluateurs (en la lisant et en la comprenant de façon détaillée). Les évaluateurs ont notamment vérifié que :

a) les mesures de sécurité physiques étaient appropriées pour protéger l'environnement de développement contre une attaque délibérée ;

b) les mesures de sécurité organisationnelles étaient adéquates pour protéger l'intégrité de la cible d'évaluation et pour maintenir la confidentialité de la documentation associée ;

c) les mesures de sécurité techniques étaient adéquates pour protéger l'intégrité de la cible d'évaluation et pour maintenir la confidentialité de la documentation associée.

5.9.16 Au cours de la phase de préévaluation, un problème dans le système de gestion de configuration a été considéré. Tout membre de l'équipe de développement pouvait modifier de façon non autorisée le code source de la cible d'évaluation produit par n'importe quel autre membre de l'équipe de développement. Le problème a été résolu en activant les fonctions de contrôle d'accès du système de gestion de configuration, de sorte que tout développeur ne puisse modifier que son propre code source.

5.9.17 Les évaluateurs ont pu visiter le site de développement et confirmer que les mesures de sécurité décrites par le commanditaire étaient appliquées, par :

a) un estimation de la conformité d'autres documentations fournies par rapport aux procédures des mesures de sécurité ;

b) un entretien avec les membres de l'équipe de développement pour vérifier s'ils étaient au courant des procédures et s'ils les appliquaient dans la pratique ;

5.9.18 Afin de vérifier plus en détail que les procédures documentées étaient appliquées, les évaluateurs ont alors :

a) vérifié les mesures de sécurité physiques en les testant. Les évaluateurs ont vérifié qu'il n'existait pas de moyen de contourner les procédures utilisées ;

b) vérifié les mesures de sécurité organisationnelles en les testant. Les évaluateurs ont vérifié la pertinence des procédures utilisées ;

c) vérifié les mesures de sécurité techniques en les testant. Les évaluateurs ont vérifié la pertinence des procédures utilisées par rapport au système de gestion de configuration outillé.

Partie 6 Conseils aux autres parties

Table des matières

Figures

Chapitre 6.1 Introduction

Objectif de cette partie

6.1.1 L'objectif de cette partie est de donner des conseils aux commanditaires, développeurs, fournisseurs, utilisateurs et responsables de l'homologation de systèmes impliqués par la sécurité des technologies de l'information (TI). Ces conseils visent à permettre à ces différents partenaires d'utiliser le plus efficacement l'ITSEM et d'obtenir une meilleure compréhension des processus d'évaluation et de certification.

6.1.2 L'utilisation efficace des TI est essentielle pour accroître la prospérité des entreprises ; le degré de dépendance des TI ainsi que la diversité de leurs utilisations dans tous les secteurs du commerce et de l'industrie ne cessent de croître. Cependant, il y a des risques potentiels associés à l'utilisation de ces technologies. Il est donc important de prendre en compte la sécurité, de préférence dès le début, et de déployer les protections appropriées. Ne pas agir ainsi peut avoir des conséquences dramatiques qui comprennent la perte de **biens**, l'atteinte à la réputation de l'entreprise, l'impossibilité de satisfaire aux exigences légales ou aux exigences du marché ou même la faillite.

6.1.3 Les utilisateurs ne sont pas toujours capables de faire une analyse détaillée de la sécurité offerte par un produit ou un système, et souhaitent fonder leur confiance sur son niveau d'assurance.

6.1.4 Pour offrir des produits et des systèmes attrayants, il est nécessaire d'introduire de nouvelles caractéristiques mais celles-ci devraient être offertes dans les meilleurs "délais de mise sur le marché" et avec un coût de production maîtrisé.

6.1.5 Les paragraphes précédents conduisent aux questions suivantes :

a) est-il utile d'offrir de la sécurité sans assurance ?

b) est-il possible d'avoir de l'assurance sans évaluation ?

c) l'évaluation peut-elle être réalisée sans un surcoût excessif ?

6.1.6 La sécurité devrait être envisagée comme une qualité naturelle de tout produit ou système, et le processus d'évaluation est le moyen par lequel le niveau d'assurance offert par la sécurité du produit ou du système peut être déterminé.

Relation entre cette partie et les autres parties de l'ITSEM

6.1.7 Cette partie est destinée à toutes les parties impliquées dans la sécurité des TI, telles que définies dans la partie 1 de l'ITSEM, et décrit les rôles et les activités respectifs dans le processus d'évaluation.

6.1.8 Des conseils spécifiques aux parties impliquées dans le processus de certification (CESSI, commanditaire et **organisme de certification**) sont fournis dans la partie 2 de l'ITSEM et dans la documentation du **schéma national**.

6.1.9 Des conseils spécifiques aux évaluateurs (les CESTI) impliqués dans le processus d'évaluation sont fournis dans la partie 4 de l'ITSEM.

6.1.10 Cette partie fournit des conseils pour les aspects de la sécurité des TI qui ne sont pas abordés par les autres parties de l'ITSEM :

a) préparation à l'évaluation : des conseils sont fournis pour assurer que les parties impliquées dans les processus d'évaluation et de certification sont convenablement préparées afin que l'évaluation soit efficace ;

b) avant ou au cours de l'évaluation : des conseils sont fournis sur le processus de développement ;

c) après l'évaluation : des conseils sont fournis sur l'utilisation des résultats de l'évaluation ;

d) après la certification : des conseils sont fournis sur l'utilisation du **certificat/rapport de certification** ;

e) après l'évaluation et la certification : les conseils fournis portent sur la modification d'un système ou d'un produit évalué.

Organisation et sommaire de cette partie

6.1.11 Cette partie se compose d'un ensemble de chapitres et d'annexes ; ces remarques préliminaires constituent le chapitre 6.1.

6.1.12 Les parties impliquées dans la sécurité des TI et leurs responsabilités sont décrites dans le chapitre 6.2.

6.1.13 Les conseils aux fournisseurs de sécurité (c'est-à-dire commanditaires, développeurs et fournisseurs) se trouvent au chapitre 6.3.

6.1.14 Les conseils aux acheteurs de sécurité (c'est-à-dire utilisateurs et responsables de l'homologation de systèmes) se trouvent au chapitre 6.4.

6.1.15 L'annexe 6.A fournit aux commanditaires et aux développeurs des conseils sur la mise à disposition des **fournitures** de l'évaluation aux évaluateurs.

6.1.16 L'annexe 6.B s'adresse aux commanditaires et aux responsables de l'homologation de systèmes et fournit un exemple de l'élaboration d'une cible de sécurité.

6.1.17 L'annexe 6.C fournit des conseils sur les mécanismes et l'estimation de l'efficacité.

6.1.18 L'annexe 6.D s'adresse aux commanditaires et aux responsables de l'homologation de systèmes et décrit l'**analyse d'impact** comme un moyen de déterminer les conséquences sur sa certification des changements apportés à un système ou à un produit évalué.

6.1.19 L'annexe 6.E fournit des conseils d'ordre général aux développeurs d'outils pour l'évaluation.

6.1.20 L'annexe 6.F s'adresse aux commanditaires, intégrateurs et responsables de l'homologation de systèmes qui sont concernés par la composition de cibles d'évaluation déjà évaluées.

Chapitre 6.2 Parties impliquées dans la sécurité des TI

Introduction

6.2.1 Les parties impliquées dans la sécurité des TI (voir la partie 1 de l'ITSEM) sont les suivantes :

a) les commanditaires, qui demandent une évaluation, définissent la cible de sécurité du produit ou du système à évaluer, supportent le coût de l'évaluation et reçoivent le certificat/rapport de certification ;

b) les développeurs (y compris les intégrateurs de systèmes) qui produisent le produit ou le système à évaluer et délivrent les fournitures requises pour l'évaluation ;

c) les CESTI qui évaluent le produit ou le système ;

d) les organismes nationaux de certification qui surveillent le processus et délivrent les certificats/rapports de certification ;

e) les fournisseurs qui vendent et distribuent des produits évalués ;

f) les utilisateurs qui se servent d'un produit ou d'un système évalué pour protéger leurs biens ;

g) les responsables de l'homologation de systèmes qui sont responsables de la sécurité d'un système évalué.

6.2.2 Il est possible qu'une même partie remplisse plus d'un rôle, par exemple en étant à la fois commanditaire et développeur, ou commanditaire et fournisseur, ou utilisateur et responsable de l'homologation de systèmes, etc.

6.2.3 Les indications spécifiques aux CESTI et aux organismes nationaux de certification sont hors du champ de cette partie.

Responsabilités des parties impliquées

6.2.4 Les objectifs des parties impliquées peuvent être classés comme suit :

a) assurer que la cible d'évaluation fournit une sécurité adéquate ;

b) réduire ou maîtriser les coûts associés à la fourniture de cette sécurité ;

c) fournir la sécurité exigée dans des délais acceptables.

6.2.5 Dans biens des cas, il est nécessaire de trouver un compromis entre ces objectifs.

6.2.6 Le commanditaire est responsable :

a) de la définition de la cible de sécurité ;

b) de la définition de la cible d'évaluation ;

c) de la mise à disposition des fournitures requises pour l'évaluation ;

d) de l'usage fait du certificat/rapport de certification ;

e) de la maintenance de la cotation de l'évaluation.

6.2.7 Le développeur est responsable :

a) de la spécification de la cible d'évaluation ;

b) du développement du produit ou du système ;

c) de la production des fournitures suivant les exigences de l'évaluation ;

d) de la maintenance du produit ou du système ;

e) de la protection de son savoir-faire et de ses informations.

6.2.8 Le fournisseur est responsable :

a) de la distribution du produit ;

b) de la publicité du produit ;

c) de fournir des conseils ;

d) de l'installation du produit.

6.2.9 L'utilisateur est responsable :

a) du choix du produit ou du système ;

b) du démarrage du produit ou du système ;

c) de l'utilisation du produit ou du système ;

d) de la configuration du produit ou du système.

6.2.10 Le responsable de l'homologation du système est chargé :

a) de la spécification de la politique de sécurité du système ;

b) de la spécification des règles de modification du système ;

c) du calcul du niveau d'assurance requis ;

d) d'approuver une exploitation du système.

6.2.11 Cette liste n'est pas définitive car différentes organisations peuvent attribuer différemment les responsabilités.

6.2.12 Un CESTI peut mener une activité de conseil dans la spécification ou la réalisation de la cible d'évaluation, mais doit s'interdire tout avis susceptible de mettre en cause son indépendance (voir le chapitre 4.2 de la partie 4).

Chapitre 6.3 Conseils aux commanditaires, développeurs et fournisseurs de sécurité

Introduction

6.3.1 Les fournisseurs de sécurité sont ceux qui produisent des données pour le processus d'évaluation (c'est-à-dire les commanditaires et les développeurs) et ceux qui fournissent des services de sécurité (c'est-à-dire les fournisseurs). Ce chapitre traite des sujets suivants :

a) la définition de la cible de sécurité (à l'attention des commanditaires) ;

b) le lancement des évaluations de produits (à l'attention des commanditaires et des fournisseurs) ;

c) la mise à disposition et la gestion des fournitures (à l'attention des commanditaires et des développeurs) ;

d) le processus de développement (à l'attention des développeurs) ;

e) les techniques spécialisées de développement (à l'attention des développeurs) ;

f) l'utilisation des RTE et des certificats/rapports de certification (à l'attention des commanditaires) ;

g) la maintenance des certificats (à l'attention des commanditaires et des développeurs) ;

h) la vente de produits certifiés (à l'attention des fournisseurs) ;

i) l'installation et la configuration de produits (à l'attention des fournisseurs) ;

j) l'intégration de produits (à l'attention des fournisseurs et des développeurs) ;

k) la fourniture de conseil (à l'attention des fournisseurs).

Définition de la cible de sécurité

6.3.2 C'est au commanditaire qu'il incombe de fournir la cible de sécurité d'une cible d'évaluation. Les objectifs d'une cible de sécurité sont les suivants :

a) fournir une spécification de la fonctionnalité de sécurité d'une cible d'évaluation ;

b) établir le lien entre une cible d'évaluation et l'environnement dans lequel il est prévu de l'exploiter ;

c) servir de base à l'évaluation.

6.3.3 L'audience visée d'une cible de sécurité peut comprendre, entre autres :

a) le développeur de la cible d'évaluation - la cible de sécurité spécifie les exigences de sécurité de la cible d'évaluation ;

b) les évaluateurs - la cible de sécurité constitue l'élément de base par rapport auquel la cible d'évaluation est évaluée ;

c) au fournisseur ou à l'utilisateur d'une cible d'évaluation - la cible de sécurité spécifie les objectifs de sécurité de la cible d'évaluation pour les responsables de la gestion, de l'achat, de l'installation, de la configuration et de l'exploitation de celle-ci.

6.3.4 Le contenu exigé par les ITSEC[1] d'une cible de sécurité (Cf. ITSEC paragraphes 2.4 à 2.26 et 4.11), déterminé selon qu'il s'agisse d'un système ou d'un produit, peut être résumé ainsi :

a) soit une politique de sécurité du système, soit un argumentaire du produit ;

b) une spécification des fonctions dédiées à la sécurité requises ;

c) une définition des mécanismes de sécurité requis (facultative) ;

d) la cotation annoncée de la résistance minimum des mécanismes ;

e) le niveau d'évaluation visé.

6.3.5 La cible de sécurité sert de base à l'évaluation et est elle-même sujet à l'évaluation.

6.3.6 L'élaboration d'une cible de sécurité pour un produit ou un système qui satisfait aux critères ITSEC exige l'application consciencieuse d'une approche méthodique. Une démarche descendante devrait notamment être adoptée pour définir une cible de sécurité, en considérant successivement :

a) les limites du domaine : l'analyse des risques ;

b) les exigences opérationnelles : la politique de sécurité ;

c) les exigences fonctionnelles : les fonctions dédiées à la sécurité ;

d) les exigences de réalisation : les mécanismes requis et la résistance minimum des mécanismes ;

e) les exigences d'évaluation : le niveau d'évaluation visé.

6.3.7 Des indications supplémentaires sur le contenu d'une cible de sécurité et une démarche descendante pour la produire sont fournies dans l'annexe 6.B.

1. NdT : ITSEC 2.4 à 2.26. La traduction a été reprise

Lancement des évaluations de produits

6.3.8 Il est souvent plus rentable d'utiliser des solutions disponibles à la vente pour satisfaire des besoins d'ordre général. Cela peut valoir autant pour des besoins de sécurité que pour tout autre besoin.

6.3.9 Un produit, vu sous l'angle de la sécurité, peut être :

a) un produit de sécurité, conçu dans le but premier, voire unique, d'avoir un usage de sécurité précis (par exemple, un produit qui réalise l'identification et l'**authentification** sur un poste bureautique) ;

b) un produit sûr, visant à offrir un niveau de sécurité déterminé en complément de sa fonctionnalité plus large (par exemple, un système d'exploitation).

6.3.10 La décision de développer et de lancer sur le marché un produit de sécurité ou un produit sûr peut reposer sur des facteurs tels que :

a) des menaces perçues par les utilisateurs qui visent leurs biens (par exemple, les attaques de virus) ;

b) des exigences légales nationales ou internationales (par exemple, *US Computer Security Act*) ;

c) des normes nationales ou internationales (par exemple, les dispositions de sécurité dans X.400 ou X.500) ;

d) un créneau du marché (par exemple, les dispositifs de contrôle d'accès pour les ordinateurs personnels).

6.3.11 Le contexte financier aura toujours un effet prépondérant dans cette décision. Le commanditaire devra répondre à un certain nombre de questions concernant la viabilité commerciale du produit. Parmi ces questions pourraient figurer les suivantes :

a) qui sont les clients potentiels ?

b) pourquoi la sécurité pose-t-elle problème à ces clients potentiels ?

c) quel niveau de sécurité (en termes de fonctionnalité et d'assurance) est nécessaire pour ces clients potentiels ?

6.3.12 Les exigences et les répercussions d'une certification du produit seront aussi abordées :

a) l'évaluation et la certification doivent-elles être recherchées dans un schéma reconnu ?

b) quel est l'impact commercial et légal d'une telle décision (par exemple, le contrôle des exportations) ?

6.3.13 Etant donné certaines hypothèses pour les points ci-dessus, le commanditaire devrait construire un plan pour son produit, qui comprennent une analyse des compétiteurs probables dans le domaine.

Mise à disposition et gestion des fournitures

6.3.14 Le commanditaire est responsable de la mise à disposition des fournitures aux évaluateurs au cours du processus d'évaluation.

6.3.15 Le terme *fourniture* est employé pour désigner tout élément (y compris la cible d'évaluation elle-même) qui doit être mis à la disposition des évaluateurs pour les besoins de l'évaluation. Cela comprend des éléments intangibles tels que l'assistance apportée aux évaluateurs (par exemple, formation en cas de besoin) et l'accès aux systèmes informatiques.

6.3.16 Les fournitures sont destinées à permettre aux évaluateurs d'évaluer la cible d'évaluation. Différents types de fourniture contribuent à cet objectif de différentes manières, entre autres :

a) les fournitures qui apportent des éléments de preuve de conformité ou d'efficacité, par exemple, une description informelle de la correspondance entre la conception détaillée et le code source ;

b) les fournitures qui permettent aux évaluateurs d'établir des éléments complémentaires de preuve de conformité ou d'efficacité, par exemple, l'accès à la cible d'évaluation développée ;

c) les fournitures qui améliorent l'efficacité globale du travail des évaluateurs, par exemple, le support technique du développeur.

6.3.17 Les commanditaires et les développeurs trouveront dans l'annexe 6.A des conseils détaillés sur le contenu et la gestion des fournitures.

6.3.18 Le commanditaire devrait s'assurer que les engagements pris par le développeur sont à la fois :

a) suffisamment fermes pour garantir que les évaluateurs disposent des fournitures demandées ;

b) suffisamment précis pour garantir que le contrat n'est pas rempli dès lors que les fournitures sont inadéquates.

6.3.19 Le commanditaire est tenu responsable de la mise à disposition des évaluateurs de toute fourniture requise, que celle-ci soit produite en sous-traitance ou associée à des produits d'un tiers (par exemple, du code source).

6.3.20 Les fournitures requises doivent être mises à disposition dans des délais raisonnables et doivent être de qualité adéquate, faute de quoi l'évaluation peut être suspendue dans l'attente de fournitures acceptables vu que ce manque peut bloquer la poursuite de l'évaluation.

6.3.21 Le développeur doit fournir toutes les fournitures prévues aux échéances déterminées d'un commun accord au début de l'évaluation. Pour remplir cette obligation, le développeur devrait :

a) confirmer l'adéquation entre son plan de développement et la liste des fournitures ;

b) confirmer l'adéquation entre les produits qui résultent de son processus de développement et la liste des fournitures ;

c) confirmer l'adéquation entre ses méthodes de développement et le niveau d'information attendu.

6.3.22 A l'occasion, le développeur peut intervenir dans l'évaluation et contribuer à la mise à disposition des fournitures au CESTI, mais il peut souhaiter limiter l'accès du commanditaire aux informations dont il a la propriété. Le développeur devrait, en temps utile, assurer que la nature et l'étendue de ces informations sont définies, et devrait établir les règles élémentaires de leur protection.

6.3.23 Avant une évaluation, le commanditaire devrait, en accord avec la législation nationale :

a) obtenir tous les droits nécessaires sur la cible d'évaluation et autres fournitures, pour l'évaluation, et accorder les droits (indemnité) au CESTI et à l'organisme de certification à ce sujet ;

b) (le cas échéant) obtenir le consentement par écrit du développeur pour toute disposition spécifique pour limiter l'accès aux informations dont il garde la propriété.

6.3.24 En conséquence de la décision de faire évaluer un produit ou un système, le développeur devrait accepter d'assumer ses responsabilités dans le processus d'évaluation.

Le processus de développement

6.3.25 Les développeurs sont censés délivrer des fournitures qui servent de preuve que le niveau d'assurance visé a été atteint (voir l'annexe 6.A). La préparation de ces éléments de preuve devrait faire partie du processus de développement ou être réalisée après le développement si l'évaluation n'était pas l'objectif initial.

6.3.26 Les critères ITSEC supposent que le processus de développement est constitué de quatre phases.

a) La phase de spécification des besoins :

pour un système, le responsable de cette phase est le commanditaire (bien que souvent le développeur d'un produit soit le commanditaire de son évaluation). Il est important pour le développeur que, durant cette phase, l'ensemble des besoins de sécurité et leur argumentaire soient clairement définis et analysés pour déterminer les forces et les faiblesses du produit ou du système proposé.

b) La phase de conception générale :

dans cette phase, les besoins de sécurité sont utilisés pour développer une architecture de sécurité et déterminer un ensemble de fonctions de sécurité. Une attention toute particulière devrait être portée à la séparation des fonctions dédiées à la sécurité et des fonctions touchant à la sécurité par rapport aux autres fonctions.

c) La phase de conception détaillée :

cette phase est un raffinement de la phase de conception générale où la fonctionnalité de chaque composant devient apparente. Une attention toute particulière devrait être portée aux forces et aux faiblesses des langages de programmation candidats au vu des fonctions et mécanismes de sécurité requis.

d) La phase de réalisation :

pendant cette phase, le développeur réalise les fonctions qui fournissent les caractéristiques de sécurité qui sont décrites dans la phase de conception détaillée. Une attention particulière devrait être portée à l'application des règles de développement, et des inspections ou des contrôles devraient faire partie de la méthode de développement ;

De plus, le développeur exécute un plan de test prédéfini. Une attention toute particulière devrait être portée à l'aspect complet du plan de test, ainsi qu'à l'enregistrement des tests effectués et des résultats correspondants, qui sont des fournitures pour l'évaluation.

6.3.27 Les conseils d'ordre général suivants sont applicables à toutes les phases énoncées précédemment comme une aide pour satisfaire pleinement les exigences des critères ITSEC :

a) les développeurs devraient adopter une approche structurée pour favoriser la production de code facile à lire, à maintenir et à tracer à travers les différents niveaux de raffinement ;

b) en analysant les informations de conception et le code source d'un composant touchant à la sécurité, un attaquant peut être capable de découvrir une manière de compromettre un objectif de sécurité. Par conséquent, les développeurs devraient protéger les informations dont ils gardent la propriété ;

c) il est recommandé aux développeurs de donner aux programmeurs une responsabilité directe sur les programmes qu'ils développent. Ceci aidera la compréhension des exigences de sécurité dans le développement ;

d) les développeurs devraient adopter un processus de revue croisée dans le processus d'identification des problèmes de sécurité et des dysfonctionnements potentiels.

Techniques de développement spécialisées

Introduction

6.3.28 Cette section fournit des conseils aux développeurs sur les techniques de développement spécialisées qui se rapportent aux niveaux d'assurance plus élevés.

Systèmes de gestion de configuration outillés

6.3.29 Pour des niveaux d'évaluation élevés, les développeurs doivent utiliser un système de gestion de configuration outillé. Cette sous-section fournit des avis pour choisir et pour développer de tels systèmes.

6.3.30 Le système de gestion de configuration devrait assurer qu'il existe une **représentation** de la cible d'évaluation claire, achevée et exacte à toutes les étapes de son cycle de vie. Cette représentation devrait refléter tous les changements qui ont été faits sur la configuration.

6.3.31 Un système de gestion de configuration outillé devrait mettre en application une politique de gestion de configuration clairement décrite, et devrait couvrir :

a) la traçabilité de toute modification de la cible d'évaluation à une demande approuvée de changement ;

b) la traçabilité de l'effet à la cause de tout dysfonctionnement de la cible d'évaluation dû à un changement ;

c) l'analyse de l'effet des changements sur les composants qui n'ont pas changé ;

d) la définition des responsabilités pour le contrôle des changements ;

e) le contrôle d'accès aux modules logiciels de la cible d'évaluation pendant leur développement ;

f) la synchronisation entre la réalisation des changements de la cible d'évaluation et la mise à jour de la documentation de la cible d'évaluation ;

g) la génération de toute version antérieure de la cible d'évaluation ;

h) l'audit des procédures de contrôle mises en place ;

i) l'audit des procédures de suivi du statut de la cible d'évaluation.

6.3.32 Il est nécessaire de fournir la confiance que la cible d'évaluation a été réalisée de façon contrôlée. Toutes les altérations de la cible d'évaluation devraient faire l'objet d'une autorisation et d'un contrôle afin de pouvoir garantir qu'elles ne nuisent pas à la capacité des composants dédiés ou touchants à la sécurité de mettre en application la politique de sécurité du système ou d'honorer l'argumentaire du produit. L'utilisation de signatures électroniques peut être efficace pour cela.

Méthodes formelles

6.3.33 L'utilisation de méthodes formelles, imposée par les critères ITSEC pour les niveaux d'évaluations élevés, présente parfois des problèmes pour les développeurs de par sa nouveauté. Cette sous-section fournit des conseils pour la sélection des techniques formelles et des outils associés.

6.3.34 *Techniques de description et de spécification formelles sous-jacentes* : au niveau E6, les critères ITSEC exigent une description formelle de la conception générale de la cible d'évaluation et une spécification formelle de ses fonctions dédiées à la sécurité.

6.3.35 En suivant les exigences E6 des critères ITSEC une comparaison formelle peut être faite entre la description formelle de la conception générale et la spécification formelle du modèle de sécurité sous-jacent. Établir cette comparaison n'est pas toujours aisé : actuellement, les techniques formelles sont aujourd'hui utilisées pour décrire et démontrer les propriétés dites statiques des cibles d'évaluation. Dans ce cas, une combinaison de techniques formelles et informelles (Cf. paragraphe E.6.6 des critères ITSEC) devient nécessaire.

6.3.36 Une autre comparaison peut être conduite entre la spécification formelle des fonctions dédiées à la sécurité et leur réalisation dans la cible d'évaluation. Une spécification formelle précise de la fonctionnalité de la cible d'évaluation est abstraite puisqu'elle implique l'utilisation d'une notation mathématique. Cette spécification est une définition sémantique ou fonctionnelle de ce que fait un système, sans indiquer comment il devrait y parvenir. Étant donnée une spécification formelle de la fonctionnalité de la cible d'évaluation, des propriétés de la cible d'évaluation peuvent être formellement exprimées et démontrées. Cette spécification est aussi une référence précise pour la réalisation.

6.3.37 Une spécification en style formel est rédigée avec une notation formelle fondée sur des concepts mathématiques bien établis (Cf. paragraphe 2.76 des critères ITSEC). La plupart des notations formelles reposent sur la logique mathématique (calcul des prédicats et plus récemment les logiques modales) et sur la théorie des ensembles.

6.3.38 Il existe trois techniques ou méthodes complémentaires pour la description formelle. Les descriptions opérationnelles utilisent un interpréteur abstrait pour définir la cible d'évaluation. Celles-ci sont les moins abstraites et ressemblent aux réalisations. Les descriptions dénotationnelles associent la cible d'évaluation directement à sa signification. Les définitions axiomatiques ou équationnelles décrivent des propriétés de la cible d'évaluation.

6.3.39 Il est recommandé que les développeurs choisissent les techniques de description et de spécification formelles en tenant compte des facteurs suivants :

a) les niveaux : pour permettre aux concepteurs ou à l'utilisateur du système de lire la description formelle à un niveau de détail plus ou moins élevé à souhait, la description devrait être faite à plusieurs niveaux allant de la description du flot de contrôle de plus haut niveau à celle des détails de chaque opération ;

b) la modularité : hormis la description formelle de plus haut niveau, toute description formelle devrait être modulaire. Cela permettra de considérer la conception de chaque opération de façon isolée ;

c) la concision : la notation devrait permettre d'exprimer les concepts nécessaires de façon concise. Une notation lourde ou verbeuse rallongera inutilement la description ;

d) la clarté : la notation utilisée pour spécifier formellement devrait être facile à comprendre ;

e) le degré d'abstraction : la description formelle ne devrait pas imposer des choix qui n'ont pas besoin d'être faits avant la phase de réalisation. Bien que le flot de contrôle de plus haut niveau soit crucial pour la conception du système, souvent l'ordre de certains événements, aux niveaux inférieurs, s'avère insignifiant ;

f) le bien fondé : la technique de description devrait avoir des bases mathématiques bien fondées afin de permettre l'élaboration de démonstrations formelles de conformité ;

6.3.40 *Outils de spécification formelle* : en bref, ce sont des outils qui mettent en œuvre - et des techniques qui utilisent - la logique mathématique. Ces techniques et outils visent à fournir une démonstration concluante que la cible d'évaluation satisfait strictement à sa spécification. Une méthode formelle outillée devra plus précisément être définie par :

a) la syntaxe et la sémantique, définies formellement, des notations utilisées ;

b) les algorithmes pour manipuler les formules des langages ;

c) l'ensemble des règles de démonstration qui permet d'inférer qu'une spécification est correcte (complétude et absence d'ambiguïté) ;

d) un cadre pour le raffinement d'une spécification en une réalisation concrète.

6.3.41 *Le caractère expressif des langages de spécification formelle* utilisés par un outil doit être suffisant pour décrire formellement la politique de sécurité et les composants d'un système TI qui la mette en application, c'est-à-dire en termes de prédicats invariants. Le langage de spécification formelle offrira des concepts qui permettent de structurer la spécification de la conception en une hiérarchie ordonnée de niveaux de spécification pour raffiner une spécification de la conception depuis la spécification de la cible d'évaluation de plus haut niveau jusqu'aux spécifications des programmes de bas niveau.

Utilisation des RTE et des certificats/rapports de certification

6.3.42 Dans certains schémas, les certificats/rapports de certification sont des déclarations officielles faites par une organisation gouvernementale et sont, par conséquent, assujetties aux règles des publications officielles. Les utilisateurs de RTE et de certificats/rapports de certification devraient prendre contact avec les organismes nationaux énumérés dans la partie 2 de l'ITSEM.

6.3.43 Le commanditaire est responsable de renoncer à ses droits sur tout résultat de l'évaluation susceptible de compromettre les informations dont le développeur garde la propriété. Si l'évaluation venait à échouer, le commanditaire devrait s'interdire d'utiliser ce résultat à l'encontre des intérêts du développeur.

6.3.44 A la fin d'une évaluation, le RTE est fourni à l'organisme de certification. Dans le processus d'évaluation et de certification, le RTE est un document provisoire et il ne représente pas la décision finale de ce processus.

6.3.45 Le RTE est communiqué au commanditaire. Il est communiqué à titre confidentiel, sans préjuger du certificat/rapport de certification officiel, étant entendu qu'il sera restreint à un cercle réduit du personnel du commanditaire et qu'il ne devrait pas être diffusé à d'autres parties sans l'accord de l'organisme de certification. Le RTE devrait porter la mention *Confidentiel évaluation.*

6.3.46 Si le commanditaire a un problème à propos d'une formulation quelconque du RTE ou du certificat/rapport de certification, il peut en débattre avec le CESTI ou l'organisme de certification selon le cas.

6.3.47 L'organisme de certification passe en revue le RTE pour déterminer dans quelle mesure la cible de sécurité est satisfaite par la cible d'évaluation et pour assurer que le CESTI a conduit l'évaluation conformément aux exigences de l'ITSEM ; il est alors en mesure de confirmer le niveau d'évaluation annoncé. Ses conclusions sont enregistrées dans le certificat/rapport de certification.

6.3.48 L'utilisation des résultats d'évaluation et des certificats/rapports de certification devrait être restreinte par les exigences spécifiques du schéma national.

Maintenance des certificats/rapports de certification

6.3.49 Un certificat/rapport de certification ne s'applique qu'à l'édition/version de la cible d'évaluation qui a été évaluée ; toute modification d'une cible d'évaluation certifiée tombe sous la coupe des procédures établies pour la réévaluation (des conseils détaillés se trouvent en annexe 6.D).

6.3.50 Le commanditaire ne peut mettre sur le marché un produit comme un produit certifié que sur la base d'un certificat/rapport de certification valide et doit garantir que des procédures de gestion de configuration adaptées au niveau d'évaluation sont mises en place afin d'empêcher les modifications non autorisées. Les évaluateurs peuvent être tenus d'archiver les données d'évaluation nécessaires à une **réévaluation**.

6.3.51 Si la cible d'évaluation ou son environnement de développement ou d'exploitation sont changés par la suite, le commanditaire a la responsabilité d'identifier le type de changement intervenu et d'en déterminer les conséquences sur le certificat/rapport de certification.

6.3.52 Le type de modification détermine si oui ou non le commanditaire doit notifier le changement à l'organisme de certification. Il se peut aussi que le commanditaire ait à demander une réévaluation.

6.3.53 Le développeur engagé dans le processus de maintenance devrait songer à mettre en place une équipe "dédiée à la sécurité" pour réaliser l'analyse d'impact de toute modification proposée ou réalisée.

6.3.54 Le processus de maintenance peut être soutenu par la politique de responsabilisation individuelle suivie au cours du développement (voir § 6.3.27.c) et peut comprendre un processus de revue consacré à la préparation des informations demandées pour la réévaluation de la cible d'évaluation, notamment :

a) un résumé des changements intervenus depuis l'édition évaluée précédente ;

b) une description de toutes les changements touchant à la sécurité et l'analyse de ces changements sur le plan de la sécurité.

6.3.55 Les commanditaires et les développeurs sont encouragés à considérer la réévaluation et la maintenance de certificat au cours du développement de la cible d'évaluation et de la préparation de l'évaluation initiale.

Commercialisation des produits certifiés

6.3.56 Les commanditaires, développeurs et fournisseurs peuvent être intéressés à la commercialisation de produits certifiés.

6.3.57 La commercialisation de produits certifiés s'accompagne des devoirs suivants :

a) fournir le certificat/rapport de certification du produit à la demande des utilisateurs potentiels ;

b) ne pas faire d'annonce trompeuse sur le produit (par exemple, une annonce que le produit est certifié alors qu'il ne l'est pas ou exagérer les bienfaits du produit) ;

c) signaler aux utilisateurs potentiels les problèmes connus dans les produits certifiés ;

d) si une **vulnérabilité** est découverte dans un produit certifié, en informer ses utilisateurs actuels ;

e) quand un produit certifié change, ne pas annoncer que le nouveau produit est certifié avant que le certificat/rapport de certification n'ait été mis à jour.

6.3.58 La cible de sécurité est le principal document intéressant pour les fournisseurs qui vendent ces produits.

Installation et configuration de produits

6.3.59 L'installation et la configuration sont généralement faites par les développeurs, les fournisseurs ou (pour des produits simples) les utilisateurs.

6.3.60 De telles installations et configurations devraient :

a) suivre avec précision les consignes de livraison du produit ;

b) choisir les options de configuration en accord à la documentation de configuration du produit, et enregistrer ce qui est fait afin que la configuration du produit soit connue dorénavant ;

c) suivre la procédure indiquée pour vérifier l'authenticité de la cible d'évaluation et se préoccuper de toute divergence découverte.

6.3.61 A cette étape, la documentation de *l'environnement d'exploitation* sera d'une grande utilité au fournisseur.

Intégration de produits

6.3.62 Il arrive fréquemment que des produits évalués doivent être intégrés ensemble dans un produit ou système composé. C'est souvent l'enjeu des produits.

6.3.63 Le développeur peut produire, s'il le souhaite, une nouvelle cible de sécurité pour le produit ou système intégré et prendre les dispositions pour une évaluation par rapport à cette nouvelle cible de sécurité. Dans ce cas, les conseils sur la **réutilisation** fournis aux chapitres 4.3 et 4.6 de la partie 4 s'appliquent. Suite à une certification réussie, le fournisseur pourra annoncer que le produit ou système intégré est certifié par rapport à la nouvelle cible de sécurité.

6.3.64 Alternativement, le fournisseur peut tout simplement contrôler que le produit ou système intégré satisfait toutes les hypothèses formulées dans les cibles de sécurité des différents produits sans décider d'une évaluation. Dans ce cas, le fournisseur peut annoncer que chacun des produits est certifié par rapport à sa cible de sécurité, mais ne peut faire aucune déclaration à propos de la cible de sécurité du système ou produit intégré. En particulier, il ne peut faire aucune déclaration sur le bon fonctionnement des produits certifiés réunis.

6.3.65 Un modèle simple pour la composition de deux composants déjà évalués est proposé en annexe 6.F. Cela intéressera ceux qui sont concernés par l'intégration de systèmes.

Fourniture d'un avis

6.3.66 Les utilisateurs qui envisagent l'acquisition de produits évalués demanderont souvent leur avis aux développeurs, fournisseurs ou CESTI.

6.3.67 La fourniture d'un avis s'accompagnent des devoirs suivants :

a) donner un avis impartial, c'est-à-dire que l'avis donné doit l'être au mieux des intérêts de l'utilisateur ; tout intérêt détenu par la personne qui donne un avis sur un produit particulier devrait être expliqué à l'utilisateur.

b) Ne pas donner d'avis en dehors du champ des compétences de la personne qui donne cet avis.

Chapitre 6.4 Conseils pour les acheteurs de sécurité

Introduction

Contexte

6.4.1 Ce chapitre fournit des conseils aux acheteurs de sécurité, c'est-à-dire aux commanditaires, aux responsables de l'homologation et aux utilisateurs de systèmes et de produits évalués. Ce chapitre traite des sujets suivants :

a) l'évaluation de la sécurité (une introduction élémentaire intéressante pour les utilisateurs) ;

b) les utilisateurs et l'évaluation (intéressant pour les utilisateurs) ;

c) la définition des besoins (intéressant pour les responsables de l'homologation de systèmes) ;

d) la recette d'un système (intéressant pour les responsables de l'homologation de systèmes) ;

e) la maintenance de l'homologation (intéressant pour les responsables de l'homologation de systèmes).

6.4.2 Ce chapitre ne vise pas à fournir une introduction générale aux concepts de la sécurité ; ces concepts sont traités dans plusieurs autres publications [GASSER]. Il se contente d'expliquer le sens d'une évaluation de la sécurité et ses conséquences pour les utilisateurs et les responsables de l'homologation de systèmes.

Utilisateurs

6.4.3 Les types suivants d'utilisateurs existent :

a) les utilisateurs finals qui utilisent un système TI pour effectuer leur travail habituel ;

b) les opérateurs, responsables du démarrage, de l'arrêt, des sauvegardes et des autres aspects routiniers liés au contrôle des systèmes ;

c) les administrateurs, responsables de la création des identifiants des utilisateurs, de la configuration du système, de l'attribution des droits d'accès aux fichiers et des fonctions similaires de contrôle de haut niveau.

6.4.4 Ces rôles impliquent différents degrés d'influence sur la sécurité d'un système TI, allant de l'absence d'influence jusqu'au caractère critique dans le maintien de la sécurité.

Responsables de l'homologation de systèmes

6.4.5 Un responsable de l'homologation d'un système est un individu, ou une organisation, qui est responsable de la sécurité d'un système, aussi bien des caractéristiques de sécurité techniques fournies par un système TI que des caractéristiques de sécurité physiques, liées au personnel et organisationnelles.

6.4.6 Les responsables de l'homologation de systèmes peuvent comprendre :

a) le propriétaire des données que contiendra le système TI qui peut avoir besoin d'une assurance quant à son caractère sûr ;

b) un agent local de sécurité, chargé de toute la sécurité TI dans une partie d'une vaste organisation ;

c) un organisme national chargé d'assurer la protection d'information importante pour la sécurité nationale.

6.4.7 Lorsqu'il estime la sécurité d'un système, le responsable de l'homologation d'un système fondera typiquement son estimation sur une politique de sécurité organisationnelle qui peut être définie pour un département ou une organisation ou quelquefois uniquement pour le système considéré. Cette politique de sécurité devrait identifier toute règle ou règlement de sécurité s'appliquant au système, y compris toute exigence non TI à mettre en application.

6.4.8 Pour établir sa confiance dans la sécurité du système, le responsable de l'homologation du système fera appel à un processus qui s'apparente à une évaluation de haut niveau, en vérifiant que la combinaison de mesures TI, physiques, liées au personnel et organisationnelles mettent effectivement en application la politique de sécurité qui s'applique au système.

6.4.9 L'évaluation technique détaillée des composants TI d'un système sera typiquement effectuée par un CESTI. Le responsable de l'homologation d'un système devra comprendre le processus d'évaluation et de certification d'un système TI suffisamment pour permettre l'exploitation des résultats de l'évaluation dans l'activité d'homologation.

6.4.10 L'implication du responsable de l'homologation d'un système dans le cycle de vie d'un système sûr intervient principalement dans trois phases :

a) au cours de la définition initiale des besoins ;

b) quand une approbation est nécessaire à la mise en service du système ;

c) chaque fois que le système est modifié ou mis à jour.

Évaluation de la sécurité

6.4.11 Il est impossible de produire des systèmes TI pratiques absolument sûrs. Ce fait est dû à la complexité des systèmes TI et à la diversité des menaces qu'ils ont à contrer.

6.4.12 Il est cependant possible de fournir une certaine confiance dans la sécurité d'un système informatique. L'approche retenue fait intervenir un organisme indépendant (appelé un centre d'évaluation de la sécurité des technologies de l'information ou CESTI) pour examiner en détail la conception et de la documentation du système à la recherche de vulnérabilités dans sa sécurité. Cet examen s'appelle une évaluation de la sécurité. L'évaluation d'un système est réussie si l'on constate que le système ne recèle pas de vulnérabilité exploitable dans sa sécurité ; autrement elle échoue.

6.4.13 Un système dont l'évaluation de sa sécurité aurait réussi, fournit vraisemblablement un certain degré de sécurité, mais il ne peut pas être considéré absolument sûr pour les raisons suivantes :

a) des vulnérabilités peuvent exister et ne pas avoir été découvertes par les évaluateurs étant donné le niveau d'information disponible aux évaluateurs ;

b) le système peut être utilisé, exploité, administré ou configuré de façon non sûre ;

c) certaines des menaces de l'environnement peuvent ne pas avoir été mises dans la cible de sécurité.

6.4.14 Il faudrait donc voir un système évalué comme jouant un rôle dans le maintien de la sécurité d'une organisation, mais sans être entièrement garant de cette sécurité. Les utilisateurs de tout type ont toujours un rôle à jouer.

Utilisateurs et systèmes évalués

Généralités

6.4.15 En ce qui concerne la sécurité, on peut considérer deux types d'utilisateurs : les utilisateurs de confiance et les autres (qui ne sont pas de confiance).

6.4.16 Les administrateurs seront généralement considérés de grande confiance car les privilèges système dont ils ont besoin pour faire leur travail et l'accès physique au système qui leur est autorisé font que la sécurité du système dépend de façon critique de l'exécution responsable de leurs devoirs.

6.4.17 Les utilisateurs finals seront généralement considérés de moindre confiance. Ils seront donc assujettis à des restrictions d'accès aux fonctions système concernant la sécurité et ils auront un rôle plus circonscrit dans le maintien de la sécurité du système.

Utilisateurs de confiance

6.4.18 Les tâches suivantes sont des exemples de tâches liées à la sécurité auxquelles les utilisateurs de confiance peuvent participer :

a) création et destruction d'identifiants d'utilisateur ;

b) configuration du système ;

c) choix des droits d'accès aux fichiers ;

d) vérification des journaux d'audit à la recherche de tentative de percées dans la sécurité.

6.4.19 Un système évalué devrait être fourni avec la documentation d'administration, de livraison, de configuration, de démarrage et d'utilisation. Au cours de l'évaluation, les évaluateurs du CESTI auront vérifié que cette documentation est exacte et que, si elle est suivie, la sécurité sera maintenue. Les utilisateurs de confiance devraient donc suivre de près cette documentation dans l'exécution de leurs tâches de sécurité.

6.4.20 Un système évalué est toujours fourni avec une cible de sécurité qui indique l'environnement nécessaire pour être sûr, en conformité avec les résultats de l'évaluation. Les utilisateurs de confiance sont chargés de maintenir cet environnement d'exploitation pour assurer le niveau d'assurance confirmé par les résultats de l'évaluation.

Autres utilisateurs

6.4.21 Les tâches suivantes sont des exemples de tâches afférentes à la sécurité auxquelles les utilisateurs qui ne sont pas de confiance peuvent participer :

a) connexion au système ;

b) déconnexion du système ;

c) choix de mots de passe ;

d) choix des droits d'accès aux fichiers qui leur appartiennent.

6.4.22 Ces tâches ne sont pas aussi critiques pour la sécurité que celles des utilisateurs de confiance mais, mal exécutées, elles peuvent mettre en péril la sécurité des données de l'utilisateur, voire celle du système dans son ensemble.

6.4.23 Un système évalué devrait être fourni avec la documentation de l'utilisateur. Au cours de l'évaluation, les évaluateurs du CESTI auront vérifié que cette documentation est exacte et que, si elle est suivie, la sécurité sera maintenue. Les utilisateurs qui ne sont pas de confiance devraient donc suivre de près cette documentation dans l'exécution de leurs tâches.

Définition des besoins

6.4.24 Au cours de l'activité de définition initiale des besoins, le responsable de l'homologation du système peut être consulté sur la politique de sécurité à appliquer ou peut être impliqué dans l'élaboration de la cible de sécurité d'un système TI.

6.4.25 Il est habituel que l'on demande au responsable de l'homologation du système à cette étape d'approuver l'approche utilisée pour le développement du système. Il est donc peut être nécessaire d'effectuer une estimation approfondie de la sécurité assez tôt dans le déroulement du projet.

6.4.26 Une estimation de la sécurité de haut niveau d'un système reposera typiquement sur les techniques d'analyse de risques, en faisant correspondre toutes les menaces possibles aux **contre-mesures** fournies. Il existe un certain nombre de techniques commercialisées ou gouvernementales qui peuvent être utilisées pour réaliser cette analyse [BDSS], [CRAMM], [GISA2], MARION et MELISA. Ces techniques s'appliquent avant tout à la sécurité fonctionnelle et fournissent peu ou pas d'indication sur le degré de confiance qu'il est nécessaire d'avoir en la conformité et l'efficacité des contre-mesures. Elles couvrent cependant certains aspects des contre-mesures de sécurité non TI qui intéressent le responsable de l'homologation du système.

6.4.27 Le responsable de l'homologation d'un système doit assurer que l'ensemble des contre-mesures identifiées par l'analyse de risques sera mis en place dans son intégralité et que ces contre-mesures œuvreront efficacement ensemble pour l'application de la politique de sécurité. Cette analyse est analogue à l'estimation de l'efficacité réalisée dans une évaluation TI selon les critères ITSEC mais comprend les contre-mesures non TI.

6.4.28 Certaines des contre-mesures seront fournies par les composants TI du système ; leurs caractéristiques de sécurité seront définies soit dans une cible de sécurité regroupant tous les aspects TI, soit dans un certain nombre de cibles de sécurité de composants isolés du système. Dans ce dernier cas, le responsable de l'homologation du système devra assurer que les différents composants TI fonctionneront efficacement ensemble dans le système.

6.4.29 Le responsable de l'homologation du système devra établir un niveau d'assurance ou de confiance requis dans la sécurité du système, en complément de la définition de la fonctionnalité de sécurité requise. Les techniques actuelles font appel à une estimation qualitative du niveau de risque du système pour attribuer un niveau de confiance requis.

6.4.30 Bien que ces lignes directrices puissent être suivies dans d'autres domaines, elles ont été développées pour des applications de type militaire et ne concernent principalement que l'aspect confidentialité de la sécurité. D'autres travaux sont nécessaires pour étendre la portée de ces lignes directrices à d'autres aspects de la sécurité et à d'autres domaines d'application.

6.4.31 Un problème particulier pour le responsable de l'homologation du système est celui de la détermination du niveau d'évaluation requis pour les composants TI d'un système, lorsque la conception du système en comprend plusieurs.

6.4.32 Les responsables de l'homologation de systèmes peuvent avoir à mettre en place des formations pour les utilisateurs de systèmes sûrs.

6.4.33 Les responsables de l'homologation de systèmes devront avoir accès à une grande variété d'informations concernant le système. Ces informations comprennent notamment :

a) les spécifications du système ;

b) la politique de sécurité du système et celles de plus haut niveau ;

c) la définition des fonctions de sécurité non TI ;

d) les cibles de sécurité des composants TI ;

e) la documentation qui concerne les procédures d'exploitation du système, y compris celles des composants TI ;

f) les certificats/rapports de certification (voire les RTE) des composants évalués au préalable.

Recette d'un système

6.4.34 Tant qu'un système est en cours de développement ou que ses composants TI sont en cours d'évaluation, des changements peuvent être proposés et des vulnérabilités peuvent être découvertes. Les problèmes rencontrés au cours de l'évaluation sont signalés en utilisant le mécanisme de **rapport d'anomalie** défini par le schéma national.

6.4.35 Les responsables de l'homologation de systèmes devront prendre en compte les implications sur la sécurité des problèmes rapportés et des modifications proposées. Une fois, la ou les évaluations terminées, le responsable de l'homologation du système devra être impliqué dans la décision de mise en exploitation du système. Dans ces deux cas, le responsable de l'homologation du système doit se prononcer sur le fait que le niveau de sécurité requis est, ou sera, atteint ou non.

6.4.36 Dans ce but, il peut être nécessaire de reprendre les éléments de l'analyse décrits dans la section précédente mais avec des informations plus précises sur la réalisation réelle ou proposée du système.

6.4.37 Le responsable de l'homologation du système devra déterminer si les **vulnérabilités exploitables** des composants TI (documentées dans le RTE) sont contrées de façon adéquate par les mesures non TI mises en place, ou si des mesures non TI supplémentaires doivent être ajoutés avant que le système ne soit mis en service.

Maintenance de l'homologation du système

6.4.38 Des changements interviendront sur la configuration, les composants et l'utilisation opérationnelle du système au cours de son exploitation. Ces changements devront être estimés par une autorité responsable de l'homologation afin de déterminer si les exigences de sécurité sont toujours satisfaites.

6.4.39 L'annexe 6.D aborde la façon de déterminer le besoin de réévaluation d'un composant TI. Une procédure analogue a besoin d'être appliquée par les responsables de l'homologation de systèmes mais étendue pour inclure les aspect non TI du système.

Annexe 6.A Fournitures de l'évaluation

Introduction

6.A.1 Cette annexe qui s'adresse plus particulièrement aux commanditaires et aux développeurs résume et explique les exigences qui concernent les fournitures ITSEC.

Responsabilités pour les fournitures

6.A.2 La responsabilité de fournir toutes les fournitures requises pour une évaluation incombe au commanditaire. Cependant, les fournitures seront, pour la plupart d'entre elles, produites et fournies par le développeur (si le commanditaire n'est pas le développeur). C'est pourquoi il est recommandé que le contrat qui lie le commanditaire au développeur contienne les détails sur ce que le développeur doit produire et quelles sont les conséquences si la production des fournitures attendues fait défaut.

6.A.3 Pour un accord particulier entre le commanditaire et le CESTI, les détails suivants peuvent avoir à être clarifiés :

a) le support et le format des fournitures informatiques ;

b) le séquencement pour la production des fournitures ;

c) le nombre d'exemplaires de fournitures à livrer ;

d) la position à adopter quant aux fournitures provisoires ;

e) les accords qui concernent les produits devant être utilisés en rapport avec la cible d'évaluation ;

f) les accords qui concernent les discussions sur l'environnement de développement avec le développeur ;

g) l'accès aux sites de développement et au site d'exploitation ;

h) le type et la durée de l'assistance du développeur, y compris l'accès aux systèmes informatiques et les besoins en locaux pour les évaluateurs.

6.A.4 Les évaluateurs auront souvent besoin d'accéder à des informations fournies par des sous-traitants ou des tierces parties. Les accords devraient prendre en compte ces cas.

6.A.5 Les frais d'envoi de toute fourniture et les risques associés (perte, dégâts dûs au feu, inondation, vol, etc.) devraient être sous la responsabilité du commanditaire, à moins qu'il en soit explicitement convenu autrement avec les évaluateurs. Il faut noter que certaines fournitures, comme de nouveaux matériels ou des matériels dédiés, peuvent ne pas avoir une valeur de remplacement facile à évaluer et peuvent présenter des risques à assurer qui ne peuvent pas être transférés aux évaluateurs.

Gestion des fournitures

Fournitures provisoires

6.A.6 Des versions stables et formalisées des fournitures sont exigées pour l'évaluation. Toutefois, il peut être parfois utile aux évaluateurs d'avoir accès à des versions provisoire de certaines fournitures, comme par exemple :

a) la documentation de test afin de permettre aux évaluateurs d'évaluer au plus tôt les tests et les procédures de test ;

b) le code source ou les schémas descriptifs de matériels afin de permettre aux évaluateurs d'estimer l'application des normes du développeur.

6.A.7 Il est plus probable que des fournitures provisoires seront fournies lorsque l'évaluation de la cible d'évaluation a lieu simultanément à son développement. Cependant, elles peuvent également être fournies au cours de l'évaluation consécutive d'un produit ou d'un système lorsque le développeur doit réaliser des développements complémentaires pour aborder des problèmes identifiés par les évaluateurs (par exemple, pour corriger une **erreur** dans la construction) ou pour fournir des éléments de preuve de la sécurité quand ils ne sont pas fournis dans la documentation existante (par exemple, des fournitures qui concernent l'efficacité lorsque le produit ou le système n'a pas été développé à l'origine pour être évalué).

6.A.8 Il est reconnu que les développeurs résistent à l'idée de remettre des fournitures provisoires aux évaluateurs. Néanmoins, c'est dans l'intérêt du commanditaire de fournir des documents provisoires de façon que le développeur puisse recevoir des observations au plus tôt sur les déficiences ou les fautes relatives à la sécurité, ce qui peut permettre de limiter l'importance de tout travail de redéveloppement ultérieur.

Contrôle de la configuration

6.A.9 Pour une évaluation au niveau E1, le commanditaire n'a besoin que de fournir une liste de configuration qui identifie la version de la cible d'évaluation à évaluer. Si le niveau d'évaluation visé est E2 ou plus, les fournitures attendues par les évaluateurs doivent également :

a) être conservées sous contrôle de configuration ;

b) être identifiées de façon unique (par exemple, par un numéro de version).

6.A.10 Cette exigence s'applique à toutes les fournitures tangibles, incluant par exemple, tous les éléments de preuves requis qui concernent l'efficacité ou la conformité, tels qu'une description de comment la conception de l'architecture de la cible d'évaluation fournit les fonctions dédiées à la sécurité de la cible de sécurité.

6.A.11 Des changements sur les fournitures devraient rester exceptionnels. Les versions révisées des fournitures doivent être envoyées aux évaluateurs le plus tôt possible.

La cible de sécurité

6.A.12 Il est de la responsabilité du commanditaire de définir ce que sera la cible de sécurité. Les objectifs de la cible de sécurité sont les suivants :

a) fournir une spécification de la fonctionnalité de sécurité d'une cible d'évaluation ;

b) décrire les liens entre une cible d'évaluation et l'environnement dans lequel il est prévu de l'exploiter ;

c) de fournir les bases pour l'évaluation.

6.A.13 La cible de sécurité s'adresse donc en particulier aux lecteurs suivants :

a) au développeur de la cible d'évaluation : la cible de sécurité définit les spécifications des besoins de sécurité de la cible d'évaluation ;

b) aux évaluateurs : la cible de sécurité constitue l'élément de base par rapport auquel la cible d'évaluation est évaluée ;

c) à l'utilisateur de la cible d'évaluation (i.e. les responsables de la gestion, de l'achat, de l'installation, de la configuration et de l'exploitation de la cible d'évaluation) : la cible de sécurité fournit toutes les informations requises pour estimer de la pertinence de la cible d'évaluation dans l'application envisagée.

6.A.14 Les exigences quant au contenu et au style de spécification de la cible d'évaluation sont déterminées par le niveau d'évaluation visé et suivant qu'il s'agit d'un système ou d'un produit. Elles peuvent être résumées comme suit :

- une politique de sécurité du système *ou* un argumentaire de produit ;
- une spécification des fonctions dédiées à la sécurité requises ;
- une définition des mécanismes de sécurité requis (optionnelle) ;
- la cotation annoncée de la résistance minimum des mécanismes ;
- le niveau d'évaluation visé.

Fournitures de l'évaluation

Généralités

6.A.15 Les exigences générales pour les fournitures sont données dans les figures 6.A.1 et 6.A.2. Cependant, certaines exigences qui concernent des fournitures additionnelles sont simplicites (plutôt qu'explicitement décrites dans les critères ITSEC). En particulier, les fournitures suivantes en relation avec l'environnement de développement global, sont habituellement demandées :

a) l'accès aux résultats d'évaluation antérieurs (par exemple, dans le cas de la réévaluation d'une cible d'évaluation ou lorsqu'un produit évalué est un composant de la cible d'évaluation) ;

b) l'accès au site de développement, incluant l'accès aux outils de développement et la possibilité de réaliser des entretiens avec certains membres de l'équipe de développement ;

c) l'accès à la cible d'évaluation dans son environnement d'exploitation ;

d) une assistance technique et logistique de la part du développeur.

6.A.16 Il n'est pas nécessaire de faire un document à part pour chaque fourniture liée à l'efficacité. Il est possible, et cela peut même être préférable dans certains cas, d'avoir un seul document couvrant tous les aspects liés à l'efficacité.

Utilisation de produits comme composants d'une cible d'évaluation

6.A.17 L'une des nombreuses approches peut être adoptée pour la mise à disposition de fournitures relatives à un produit qui constitue un composant dédié ou touchant à la sécurité. On peut citer par exemple :

a) les résultats d'une évaluation précédente du produit ;

b) le produit peut être traité de la même façon que le reste de la cible d'évaluation auquel cas, les fournitures appropriées relatives au produit devraient être fournies.

6.A.18 L'approche adoptée pour une évaluation donnée doit être acceptable pour l'organisme de certification, le commanditaire et les évaluateurs. On trouvera des conseils complémentaires dans le chapitre 4.6 de la partie 4 si des résultats d'évaluation existants doivent être réutilisés.

Environnement de développement

6.A.19 Les évaluateurs devront disposer de la documentation relative au contrôle de configuration, aux langages de programmation, aux compilateurs et à la sécurité des développeurs utilisée ou appliquée au cours du développement de la cible d'évaluation. Les évaluateurs devront également disposer de la documentation relative plus généralement aux procédures, méthodes, normes et outils utilisés au cours du développement de la cible d'évaluation comme par exemple :

a) le plan qualité qui contient les procédures de développement ;

b) des détails sur les méthodes de développement utilisées ;

c) des détails sur les outils de développement utilisés ;

d) les normes de programmation du logiciel.

6.A.20 Les évaluateurs devront demander des éléments de preuve qui démontrent le respect des procédures et normes et les éléments de preuve que les outils et les méthodes ont été correctement utilisés comme par exemple :

a) le plan de gestion de configuration ;

b) les enregistrements de contrôle de configuration ;

c) les minutes des revues de conception.

6.A.21 Les évaluateurs peuvent également demander à faire une ou plusieurs visites spécifiques pour s'entretenir avec les développeurs à propos de l'environnement de développement. Les sujets à aborder lors de ces visites sont énumérés dans le tableau de la figure 6.A.3.

6.A.22 Les évaluateurs n'ont pas de droit d'accès aux informations purement financières, contractuelles ou liées au personnel (autres que les questions relatives au personnel sur lesquelles porte les critères ITSEC concernant la sécurité des développeurs).

Environnement d'exploitation

6.A.23 Les évaluateurs devront disposer de la documentation relative à l'utilisation, l'administration, la livraison, la configuration, au démarrage et à l'exploitation de la cible d'évaluation.

6.A.24 Les évaluateurs demanderont l'accès à la cible d'évaluation opérationnelle afin d'effectuer des tests de pénétration. Si la cible d'évaluation est un système, les évaluateurs demanderont également l'accès au site opérationnel, si possible afin de :

a) s'entretenir avec les représentants des utilisateurs à propos des procédures opérationnelles;

b) d'effectuer des tests de pénétration dans l'environnement d'exploitation.

6.A.25 Si la cible d'évaluation est un produit, les évaluateurs demanderont l'accès à une réalisation opérationnelle du produit afin d'effectuer des tests de pénétration. Le commanditaire peut faire en sorte que la cible d'évaluation soit disponible sur le site de développement ou que les équipements nécessaires puissent être empruntés par les évaluateurs afin d'exécuter les tests de pénétration dans le CESTI.

Assistance pour l'évaluation

6.A.26 Les évaluateurs peuvent demander une assistance en termes de logistique, de conseil ou de formation de la part du commanditaire et du développeur au cours d'une évaluation.

6.A.27 Une personne désignée dans l'organisme du développeur devrait servir d'interlocuteur pour toutes les actions d'assistance de la part du développeur. Cette personne, ou les personnes alternativement désignées :

a) devraient être à même de fournir une assistance de manière opportune ;

b) devraient être à même d'assurer la liaison avec d'autres membres de l'équipe de développement, quand des informations détaillées sont attendues pour des aspects particuliers de la cible d'évaluation.

6.A.28 L'effort d'assistance sera fonction de chaque évaluation. Les facteurs affectant cet effort prendront en compte le niveau d'évaluation visé, la taille et la complexité du système et l'expérience du développeur ou du commanditaire dans le développement de système ou de produits évalués. Certains aspects du processus d'évaluation tels que la réalisation de tests sur la cible d'évaluation demandent une assistance plus soutenue.

6.A.29 Les types d'assistance demandée pourraient comprendre :

a) la formation ;

b) les entretiens informels ;

c) l'accès et l'assistance aux systèmes informatiques ;

d) les locaux.

6.A.30 Une formation informelle, dispensée de préférence par un membre de l'équipe de développement, peut être nécessaire sur un certain nombre des domaines qui sont la propriété du développeur et pour lesquels la documentation est peu répandue tels que :

a) le matériel et (le ou) les systèmes d'exploitations utilisés dans la cible d'évaluation et pour son développement ;

b) les méthodes de développement utilisées ;

c) les outils de développement utilisés.

6.A.31 Le développeur n'est normalement pas tenu d'organiser une formation rigoureuse pour les évaluateurs. Toutefois, les évaluateurs peuvent souhaiter participer aux cours de formation dispensés à l'attention d'autres personnes comme par exemple :

a) lorsqu'une formation est dispensée à une équipe de développement portant par exemple sur une méthode de développement particulière ;

b) lorsqu'une formation est organisée au profit des utilisateurs portant par exemple sur l'administration de la sécurité de la cible d'évaluation.

6.A.32 Des entretiens informels avec le développeur peuvent être nécessaires sur n'importe quel aspect de la cible d'évaluation. Typiquement, les évaluateurs peuvent demander au développeur de fournir de courtes descriptions sur un aspect particulier de la cible d'évaluation, et de répondre ensuite aux questions qu'ils poseraient.

6.A.33 Les évaluateurs devront avoir accès aux systèmes informatiques appropriés, principalement pour effectuer des tests sur la cible d'évaluation. Les "systèmes informatiques" dans ce contexte incluent tout équipement utilisé par le développeur pour réaliser la cible d'évaluation et la tester.

6.A.34 Si la cible d'évaluation est un système, les évaluateurs devront également, si cela est possible, avoir accès aux systèmes informatiques utilisés pour l'exploitation de la cible d'évaluation (voir les paragraphes 6.A.23 à 6.A.25).

6.A.35 Les évaluateurs devront avoir un accès dédié au système informatique pour quelque temps lors de l'exécution des tests complémentaires (à ceux du développeur) ou des tests de pénétration.

6.A.36 La durée d'accès au système informatique dépendra de la nature de la cible d'évaluation.

6.A.37 L'accès au système informatique a normalement lieu sur le site de développement ou le site d'exploitation. Dans certains cas, cependant, il peut être commode de fournir l'accès dans un autre lieu, par exemple, en fournissant le système informatique au CESTI.

6.A.38 Quand les évaluateurs utilisent un système informatique, une assistance peut être demandée pour certaines opérations de base telles que le démarrage du système informatique, la réalisation de copies de sauvegardes de la cible d'évaluation, l'exécution de tests, etc.

6.A.39 Un bureau à l'usage exclusif des évaluateurs devrait être obtenu à leur demande lorsque les évaluateurs travaillent sur le site de développement ou sur le site d'exploitation. Ce bureau devrait être en mesure d'accueillir le nombre requis de personnes et devrait inclure :

a) le mobilier de base, y compris un téléphone ;

b) des moyens de stockage sûr en fonction du niveau de classification des informations propre à la cible d'évaluation.

6.A.40 Il arrive que le règlement intérieur de certains sites interdisent l'accès non accompagné au site de développement ou au site opérationnel. Cependant, les évaluateurs auront besoin d'être isolés de temps en temps lorsqu'ils travailleront sur le site. Des modalités devront donc être définies pour permettre aux évaluateurs d'être non accompagnés lorsqu'ils seront dans ce bureau.

Figure 6.A.1 Fournitures de l'évaluation (efficacité)	
FOURNITURES	**TOUS LES NIVEAUX D'ÉVALUATION**
Analyse de pertinence : **une investigation qui montre que les fonctions et les mécanismes dédiés à la sécurité de la cible d'évaluation contreront effectivement les menaces pour la sécurité de la cible d'évaluation identifiées dans la cible de sécurité**	✔
Analyse de cohésion : **une investigation qui montre que les fonctions et les mécanismes dédiés à la sécurité coopèrent pour former un ensemble intégré et efficace**	✔
Analyse de la résistance des mécanismes **une investigation qui montre la capacité de la cible d'évaluation considérée dans son ensemble à contenir une attaque directe tirant profit d'insuffisances dans ses algorithmes, ses principes ou ses propriétés sous-jacents ; cette estimation exige de prendre en considération le niveau des ressources qui serait nécessaire à un agresseur pour réussir une attaque directe**	✔
Liste des vulnérabilités connues dans la construction **une liste des vulnérabilités potentielles dans la construction de la cible d'évaluation (identifiées par le développeur) plus un argumentaire qui expliquent pourquoi elles ne sont pas exploitables**	✔
Analyse de la facilité d'emploi **une investigation qui montre que la cible d'évaluation ne peut pas être configurée ou utilisée d'une manière qui n'est pas sûre mais qu'un administrateur ou un utilisateur final pourrait raisonnablement croire sûre**	✔
Liste des vulnérabilités connues en exploitation **une liste des vulnérabilités potentielles dans l'exploitation de la cible d'évaluation (identifiées par le développeur) plus un argumentaire qui explique pourquoi elles ne sont pas exploitables**	✔

Figure 6.A.2 Fournitures de l'évaluation (conformité)

FOURNITURES	NIVEAU D'ÉVALUATION					
	E1	E2	E3	E4	E5	E6
Spécification des besoins						
La cible de sécurité de la cible d'évaluation	✔	✔	✔	✔	✔	✔
La définition ou la référence à un modèle sous-jacent de sécurité spécifié de façon formelle				✔	✔	✔
L'interprétation informelle du modèle sous-jacent sous l'angle de la cible de sécurité				✔	✔	✔
Conception générale						
La description informelle de la conception générale de la cible d'évaluation	✔	✔	✔			
La description semi-formelle de la conception générale de la cible d'évaluation				✔	✔	
La description formelle de la conception générale de la cible d'évaluation						✔
Conception détaillée						
La description informelle de la conception détaillée		✔	✔			
La description semi-formelle de la conception détaillée				✔	✔	✔
Réalisation						
La documentation de test	(✔)	✔	✔	✔	✔	✔
La bibliothèque des programmes de test et les outils utilisés pour tester la cible d'évaluation	(✔)	✔	✔	✔	✔	
La bibliothèque des programmes de test et les outils utilisés pour tester la cible d'évaluation, y compris les outils qui peuvent être utilisés pour détecter les incohérences entre le code source et le code exécutable, dans le cas où il existe des composants sous forme de code source, dédiés à la sécurité ou touchant à la sécurité (par exemple un désassembleur ou un outil de mise au point).				✔		✔
Le code source ou les schémas descriptifs des matériels de tous les composants dédiés à la sécurité ou touchant à la sécurité			✔	✔	✔	✔
La description informelle de la correspondance entre le code source ou les schémas descriptifs des matériels et la conception détaillée.			✔		✔	
La description informelle de la correspondance entre le code source ou les schémas descriptifs des matériels et la conception détaillée, ainsi que la spécification formelle des fonctions dédiées à la sécurité						✔

Note: (✔) - fourniture optionnelle

Figure 6.A.2 Fournitures de l'évaluation (conformité)

FOURNITURES	NIVEAU D'ÉVALUATION					
	E1	E2	E3	E4	E5	E6
Contrôle de la configuration						
La liste de configuration identifiant la version de la cible d'évaluation à évaluer	✔	✔	✔	✔	✔	✔
Des informations sur le système de gestion de configuration		✔	✔			
Des informations sur le système de gestion de configuration et les outils associés				✔	✔	✔
Des informations d'audit sur les modifications de toutes les parties de la cible d'évaluation soumises à la gestion de configuration				✔		
Des informations d'audit sur les modifications de tous les objets de la cible d'évaluation soumises à la gestion de configuration					✔	✔
Des informations sur la procédure de réception			✔	✔	✔	✔
Des informations sur la procédure d'intégration					✔	✔
Langages de programmation et compilateurs						
La description de tous les langages de programmation utilisés			✔	✔	✔	✔
La description de tous les compilateurs utilisés				✔	✔	✔
Le code source de toutes les bibliothèques de routines système utilisées					✔	✔
Sécurité des développeurs						
Des informations sur la sécurité de l'environnement de développement		✔	✔	✔	✔	✔
Exploitation						
La documentation utilisateur	✔	✔	✔	✔	✔	✔
La documentation d'administration	✔	✔	✔	✔	✔	✔
La documentation de livraison et de configuration	✔	✔	✔	✔	✔	✔
La documentation de démarrage et d'exploitation	✔	✔	✔	✔	✔	✔

Figure 6.A.3 Sujets d'entretien concernant l'environnement de développement

GESTION DE CONFIGURATION DU DÉVELOPPEMENT

Champ : Les procédures (manuelles et automatisées) pour le contrôle et la traçabilité des données d'un projet

Sujets : Organisation informatique
- Structure des répertoires
- Bibliothèques logiciel et contrôle d'accès

Contrôle des modifications
Procédures de diffusion

LANGAGES DE PROGRAMMATION ET COMPILATEURS

Champ : Les langages de programmations utilisés pour la réalisation

Sujets : Définition des langages
Options dépendant de leur réalisation
Compilateurs

SÉCURITÉ DU DÉVELOPPEMENT

Champ : Sécurité de l'environnement de développement c'est-à-dire, protection de la cible d'évaluation et confidentialité des documents associés

Sujets : Mesures physiques
Mesures organisationnelles
Mesures liées au personnel

MÉTHODES DE DÉVELOPPEMENT

Champ : Les différentes phases de développement et l'approche adoptée

Sujets : Historique du projet et état courant
Représentations produites
Processus de conception
Phase de codage
Stratégie de test

OUTILS DE DÉVELOPPEMENT

Champ : Les outils (dont le développeur a la propriété et construits pour l'occasion) utilisés durant le développement

Sujets : Machines de développement, administration du système
Compilateurs/éditeurs de liens/outils de mise au point
Procédure de génération du système
Programmes de test

PROCÉDURES DE DÉVELOPPEMENT

Champ : Les contrôles appliqués au cours du développement

Sujets : Procédures de gestion de projet
Procédures d'assurance qualité
Procédures de contrôle technique

NORMES DE DÉVELOPPEMENT

Champ : Les normes utilisées au cours du développement

Sujets : Normes de conception
Normes de programmation
Normes de documentation

Annexe 6.B Rédaction d'une cible de sécurité

Introduction

6.B.1 Cette annexe présente des conseils au commanditaire d'une évaluation pour la rédaction d'une cible de sécurité. En guise d'exemple, une description est présentée sur la manière dont la cible de sécurité du système SWAN (décrite en partie 5 de l'ITSEM) pourrait être réécrite.

L'objectif d'une cible de sécurité

6.B.2 Lors de la création d'une cible de sécurité, le commanditaire a pour objectif la fourniture d'une base, complète et cohérente, à utiliser au cours de l'évaluation. La cible de sécurité est un document exhaustif (ou un ensemble de documents) qui dicte entre autres :

a) les objectifs de sécurité du produit ou du système (cible d'évaluation) ;

b) les contre-mesures employées par la cible d'évaluation pour traiter les menaces perçues.

6.B.3 A cette fin, une cible de sécurité présente les exigences de sécurité de la cible d'évaluation décrites à un haut niveau d'abstraction.

6.B.4 De plus, la cible de sécurité forme une partie de la base contractuelle entre le commanditaire et le CESTI car elle spécifie des informations, telles que le niveau d'évaluation, qui restent pertinentes pendant toute la durée de l'évaluation.

6.B.5 Du point de vue du développeur, la cible de sécurité fait partie intégrante de la spécification de haut niveau de la cible d'évaluation. A cette fin, les développeurs exigent de la cible de sécurité qu'elle précise sans ambiguïté les caractéristiques et les utilisations possibles de la cible d'évaluation.

6.B.6 La cible de sécurité peut contenir des aspects organisationnels, fonctionnels et techniques. Elle peut également aborder d'autres aspects imposés par les spécifications de besoin, tels que l'assistance.

6.B.7 La cible de sécurité constitue une spécification pour les parties dédiées à la sécurité de la réalisation. La cible de sécurité devrait être écrite le plus tôt possible dans le cycle de vie du développement afin de permettre à une évaluation simultanée de démarrer au plus tôt. Cependant cela n'est possible que si la cible de sécurité est suffisamment stable.

6.B.8 Bien que les exigences de sécurité soient spécifiées séparément dans la cible de sécurité, le raffinement des exigences de sécurité et de celles qui ne le sont pas est réalisé simultanément.

6.B.9 Pour une évaluation consécutive, si la cible d'évaluation a été développée avant que la cible de sécurité ne soit rédigée, il sera nécessaire de faire un travail de "rétro-conception" pour toute l'information exigée.

6.B.10 Bien que le commanditaire soit responsable de la fourniture de la cible de sécurité aux évaluateurs, il peut ne pas être un expert sur tous les aspects de la sécurité. Il est de ce fait recommandé que le commanditaire soit assisté lors de la rédaction d'une cible de sécurité. Une telle assistance peut être fournie par les développeurs qui sont biens placés pour produire la spécification qu'ils devront réaliser. Néanmoins, un CESTI pourrait également être consulté pour fournir des conseils qui ont trait au contenu et à la présentation de la cible de sécurité.

6.B.11 Pour les acquéreurs d'un système (i.e. les utilisateurs dont les besoins sont à satisfaire par la conception du système), la cible de sécurité devrait fournir les éléments de base leur permettant de prendre leurs décisions d'acquisition.

6.B.12 Il est de la responsabilité des évaluateurs de déterminer si la cible d'évaluation est cohérente avec la cible de sécurité. De plus, les évaluateurs doivent estimer si la spécification de la cible d'évaluation est valide au regard des autres fournitures de l'évaluation.

Le contenu d'une cible de sécurité

6.B.13 Pour remplir son rôle dans une évaluation, une cible de sécurité doit :

a) détailler les spécifications des besoins de sécurité de la cible d'évaluation ;

b) présenter les contre-mesures proposées pour contrer les menaces identifiées portant sur les biens protégés par la cible d'évaluation.

6.B.14 Dans ce but, les critères ITSEC imposent :

a) que les exigences de sécurité soient couvertes par une politique de sécurité (pour les systèmes) ou un argumentaire (pour les produits) ;

b) que des fonctions soient conçues pour satisfaire les exigences de sécurité ; elles sont appelées fonctions dédiées à la sécurité ;

c) que dans le cas où une solution technique particulière est imposée pour satisfaire une exigence de sécurité, par exemple, l'utilisation d'un algorithme particulier de chiffrement de mots de passe, cette solution doit être mentionnée comme un mécanisme de sécurité requis ;

d) qu'une cotation minimum de la résistance des mécanismes qui doit être *élémentaire, moyenne, élevée*, soit annoncée ;

e) qu'un niveau d'évaluation visé par la cible d'évaluation soit spécifié.

6.B.15 On notera que les fonctions dédiées à la sécurité peuvent devoir être spécifiées dans un style semi-formel ou formel suivant le choix du niveau d'évaluation.

Analyse de risque

6.B.16 La spécification des fonctions dédiées à la sécurité impose un compromis entre la nécessité de protéger les biens et le coût d'une telle protection (par exemple, en termes financier, opérationnel, technique et de ressources humaines). Ce compromis est contrôlé par un processus d'analyse de risque.

6.B.17 De plus, la construction d'une cible d'évaluation aborde à la fois les exigences propres à la cible d'évaluation et toutes les autres contraintes applicables (par exemple les lois, les instructions, la technologie, les biens, les coûts, etc.).

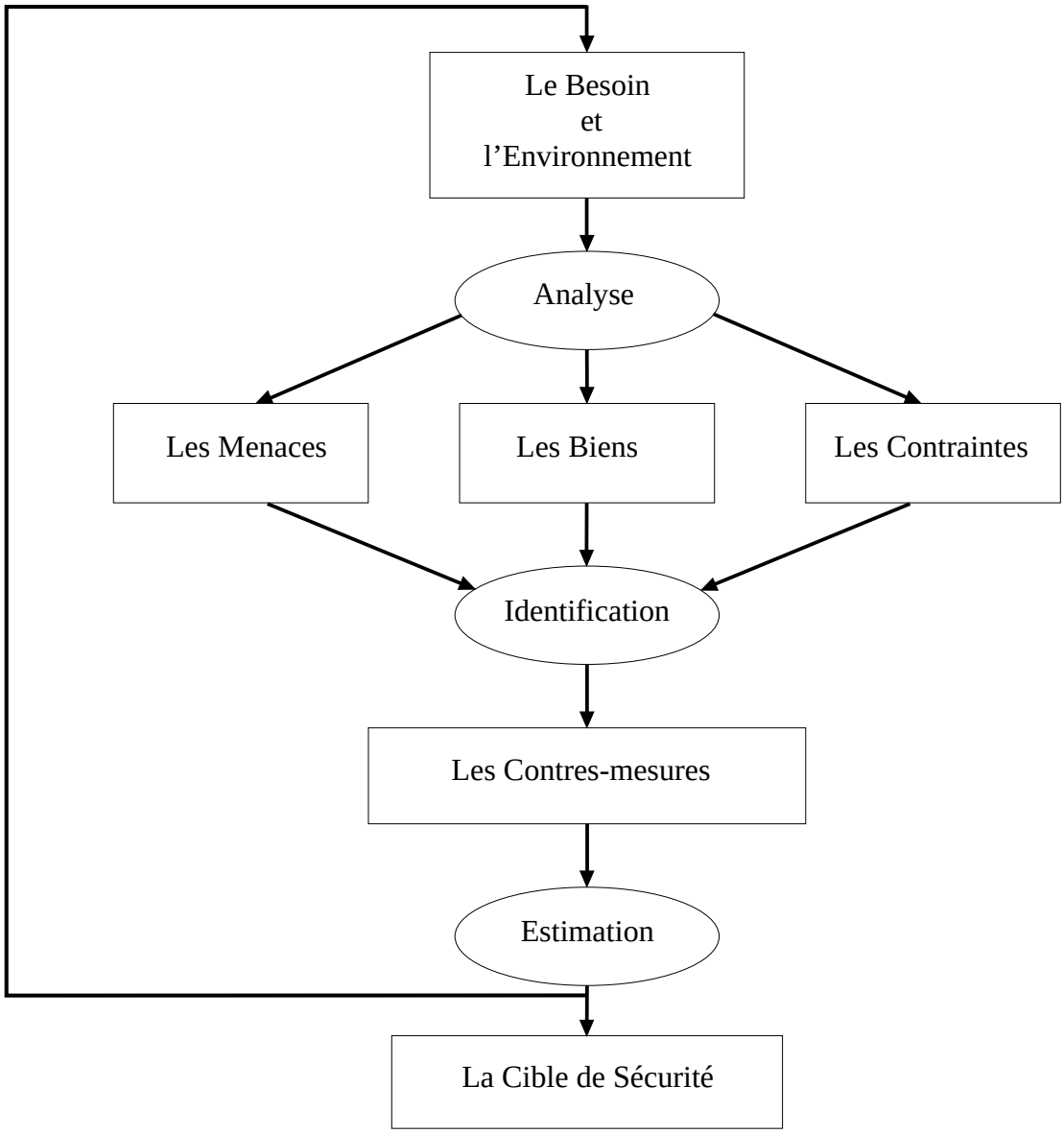


Figure 6.B.1 Approche pour l'analyse de risque

6.B.18 L'analyse de risque détermine les menaces sur les biens protégés par la cible d'évaluation. Pour chaque menace, on estime la probabilité pour qu'un bien soit compromis.

6.B.19 L'analyse de risque devrait être une des premières activités réalisée dans le développement de la cible d'évaluation.

6.B.20 Cependant, le développement est rarement un processus linéaire si bien que des révisions périodiques et des changements de la cible de sécurité sont probables. De tels changements sont un problème pour les évaluateurs car ils invalident souvent les résultats de l'évaluation.

6.B.21 Le processus d'analyse de risque guide la production de la cible de sécurité abordant tour à tour les biens, les menaces et les contre-mesures afin de produire finalement la cible de sécurité.

6.B.22 L'analyse de risque consiste en une succession d'activités qui portent sur les spécifications et les exigences (voir la figure 6.B.1), à savoir :

a) l'analyse du problème (par rapport à l'environnement et aux besoins) ;

b) l'identification des choix possibles (par rapport aux biens, aux menaces et aux contraintes) ;

c) l'estimation d'une solution (par rapport à la pertinence, à la faisabilité et aux coûts des contre-mesures) ;

d) la prise en compte de la décision (par rapport aux choix et au bilan).

6.B.23 Des variantes de ce processus sont décrites dans des méthodes standard ([CRAMM], MARION, MELISA, [GISA2]). Elles sont très utiles pour la production de répertoires de ressources, menaces et classes de contre-mesures.

6.B.24 En l'absence d'une méthode, il peut être approprié d'utiliser des spécifications génériques. Les classes de fonctionnalité pré-définies des critères ITSEC et les modèles de sécurité pour les systèmes ouverts de l'ISO en sont des exemples.

Politique de sécurité d'un système ou argumentaire d'un produit

Généralités

6.B.25 La cible de sécurité commence par l'énoncé des menaces, des objectifs et de l'environnement de la cible d'évaluation. Pour un système, on trouve cet énoncé dans sa politique de sécurité. Pour un produit,dans un argumentaire.

6.B.26 La politique de sécurité ou l'argumentaire du produit établit qui peut faire quoi avec les équipements, les services, les fonctions et les dispositifs de la cible d'évaluation.

6.B.27 La production d'une politique de sécurité d'un système ou de l'argumentaire d'un produit destinés à être utilisés dans une cible de sécurité peut être difficile. Une politique de sécurité ou l'argumentaire d'un produit devrait exposer les biens devant être protégés et les règles régissant le traitement des biens sans tenir compte de la conception de la cible d'évaluation.

Environnement prévu

6.B.28 Une étude de la cible d'évaluation et de l'environnement dans lequel elle opérera, qui contient l'analyse de risque des aspects de sécurité de la cible d'évaluation, définit les caractéristiques opérationnelles de la cible d'évaluation. Ces caractéristiques déterminent comment la cible d'évaluation s'interface avec son environnement et par conséquent, comment elles doivent être décrites dans la cible de sécurité.

6.B.29 Cette section de la cible de sécurité devrait définir :

a) le but et les limites de la cible d'évaluation ;

b) l'information qui doit être traitée par la cible d'évaluation et comment elle doit l'être ;

c) les personnes qui utilisent la cible d'évaluation (par exemple, les utilisateurs, les opérateurs, les administrateurs, etc.) ;

d) l'équipement nécessaire pour permettre l'exploitation de la cible d'évaluation ;

e) la localisation et la topologie de la cible d'évaluation, y compris les mesures de sécurité physique ;

f) les modes d'exploitation et les procédures ;

g) l'organisation et ses procédures.

Le système SWAN : environnement prévu

6.B.30 Le SWAN (*Site-Wide Area Network*) est un réseau de communication qui permet à plusieurs communautés d'utilisateurs d'accéder à différentes applications de traitement de données.

6.B.31 Cet exemple de système se trouve sur un site étendu appartenant à une organisation commerciale. Ce site est complètement clôturé par une barrière couvrant son périmètre qui est bien surveillée. L'ensemble du personnel a été minutieusement contrôlé par l'organisation et est digne de confiance. Les visiteurs du site sont accompagnés en permanence.

6.B.32 On trouve sur ce site des zones disposant de protections supplémentaires sous la forme d'un contrôle d'accès physique et de procédures de sécurité spécifiques. Les menaces cryptographiques et de type TEMPEST sont faibles. Les terminaux sont situés dans des zones sécurisées et les utilisateurs autorisés empêcheront les visiteurs d'utiliser un terminal sans supervision se trouvant dans une pièce.

6.B.33 Sur ce site, se trouve une grande variété de systèmes TI différents, acquis à différentes époques provenant de différents fournisseurs et utilisés pour divers usages tels que la gestion transactionnelle, la facturation ou l'administration de la société.

6.B.34 Les connexions entre les terminaux utilisateurs et les systèmes hôtes, qui peuvent être situés dans des bâtiments différents, ont auparavant été réalisées avec des cables spécifiques en fibre optique. Ces connexions sont maintenant remplacées par le SWAN. Le SWAN est un réseau TCP/IP sur un anneau à jeton constitué d'une double boucle contrarotative et de plusieurs sous-anneaux. Un équipement d'un système d'extrémité est raccordé au SWAN par des points d'accès pour hôte ou par des points d'accès pour terminal.

6.B.35 Les systèmes hôtes sont utilisés soit en mode dédié soit en mode dominant, par exemple, Confidentiel Entreprise, Confidentiel Administration ou Confidentiel Direction.

6.B.36 Les droits d'accès sont définis pour chaque utilisateur. L'ensemble du personnel du site est soit autorisé à accéder au moins à l'information classifiée Confidentiel Entreprise, soit accompagné par du personnel autorisé.

6.B.37 Les procédures d'utilisation proviennent d'une configuration antérieure ou chaque serveur était le pivot d'un réseau spécifique. En conséquence, l'accès aux applications mises en œuvre par chaque système hôte est géré localement sur une base discrétionnaire par un gestionnaire d'application.

6.B.38 Comme chaque terminal et système hôte peuvent fonctionner à différents niveaux de sécurité, l'administrateur du système a établi une politique de contrôle d'accès obligatoire pour relier les terminaux aux serveurs dans la nouvelle version de SWAN.

Objectifs de sécurité

6.B.39 La première étape dans l'établissement d'une politique de sécurité est de déterminer les objectifs de sécurité. Les objectifs de sécurité sont exprimés en terme de :

a) biens de l'organisation qui nécessite une protection, que ce soit par la cible d'évaluation, un autre système ou peut-être par des moyens physiques / manuels ; les biens incluent l'information devant être traitée par la cible d'évaluation, les processus devant être automatisés par la cible d'évaluation et les responsabilités ou rôles des utilisateurs.

b) ressources de la cible d'évaluation telles qu'elles sont définies dans les spécifications externes ; les ressources peuvent être les ressources physiques, par exemple les équipements ou les périphériques, ou des ressources abstraites telles que la configuration de la cible d'évaluation, des processus, des algorithmes ou du code.

6.B.40 L'analyse de risque tient compte du niveau de sécurité traduit dans les objectifs de sécurité (par exemple, dans le cas de la confidentialité des données, quelle classification peut être protégée). L'évaluation ne prend pas ces aspects en considération mais se concentre plutôt sur la confiance que l'on peut avoir dans la réalisation des fonctions dédiées à la sécurité. Par conséquent, la cible de sécurité ne devrait pas faire référence à ce degré de protection.

6.B.41 Deux approches sont possibles lorsque l'on considère les objectifs de sécurité :

a) toutes les données et les ressources sont analysées les unes après les autres en considérant tous les objectifs de sécurité pertinents ;

b) les ressources et les données relatives au même objectif de sécurité sont regroupées ensemble pour l'analyse.

6.B.42 Les objectifs de disponibilité sont décrits en terme d'état, de capacité, de durée de service, de temps de réponse, de priorités et de tolérance à la dégradation.

6.B.43 Les objectifs d'intégrité s'inscrivent dans :

a) la conformité à des normes, des spécifications et des références ;

b) la conformité à un état initial ou à une condition ;

c) des règles qui doivent être observées pour l'uniformité et la cohérence.

6.B.44 Les objectifs de confidentialité expliquent l'utilisation attendue de chaque ressource plutôt que d'aborder les vulnérabilités à éviter (par exemple, la divulgation, la substitution de contexte, le détournement d'un objectif).

6.B.45 L'auteur de la cible de sécurité doit s'efforcer de rendre cette section aussi exhaustive que possible car les objectifs de sécurité forment en définitive la base de l'évaluation. On ne peut considérer comme dédiée à la sécurité, une caractéristique de la cible d'évaluation qui ne peut être attribuée à un objectif de sécurité.

Le système SWAN : objectifs de sécurité

6.B.46 Les biens de l'organisation à protéger sont les services applicatifs fournis à chaque communauté d'utilisateur. Il n'y a pas d'objectif de sécurité pour les ressources du système.

6.B.47 Ces services (informations et traitements) ne doivent pas être accessibles à des personnes extérieures à la communauté.

6.B.48 Il n'y a pas d'objectif de disponibilité.

6.B.49 Il n'y a pas d'objectif d'intégrité ce qui implique qu'une attaque contre l'intégrité des services fournis à chaque communauté d'utilisateur n'est pas redoutée ou qu'une attaque est tolérable tant que la confidentialité des services n'est pas menacée.

6.B.50 L'utilisation incorrecte des services applicatifs par les utilisateurs autorisés n'est pas prise en compte.

Les menaces

6.B.51 L'étape suivante dans l'établissement d'une politique de sécurité est de déterminer les menaces identifiées sur les biens, i.e. les actions qui pourraient violer les objectifs de sécurité.

6.B.52 Comme c'était le cas pour les objectifs de sécurité, les menaces sont un résultat à prendre en compte durant la spécification de la cible d'évaluation. Comme suggéré ci-dessus, elles dépendent de la description externe de la cible d'évaluation. Cependant, il est plus difficile de déterminer les menaces que de fixer les objectifs de sécurité du fait qu'il est impossible de traiter tous les modes d'attaque possibles.

6.B.53 Les méthodes d'analyse du risque peuvent aider à l'estimation des menaces, pas tant pour les procédés systématiques employés que pour la connaissance que l'on peut en obtenir. Ces techniques peuvent fournir une liste de menaces génériques qui peuvent être immédiatement appliquées à la cible d'évaluation en question. Cette méthode peut apporter des conseils pertinents pour estimer les menaces, estimation qui peut être fondée sur les événements ou sur les objectifs selon les exigences de l'analyste.

6.B.54 Les auteurs de la cible de sécurité devraient noter qu'ils sont responsables de l'exactitude et de la complétude des objectifs de sécurité et des menaces. Les évaluateurs ne peuvent vérifier la complétude de ces informations mais en vérifieront l'exactitude et la cohérence.

Le système SWAN : Les menaces

6.B.55 Au cours de l'analyse de risque, différents types de menaces ont été considérés tour à tour :

a) des attaques physiques contre le système et son environnement ;

b) l'interception du rayonnement compromettant ;

c) l'attaque directe des applications.

6.B.56 Les attaques physiques ne s'appliquent pas aux systèmes hôtes ou aux terminaux qui sont gardés ou surveillés en permanence, mais aux câbles du réseau pouvant faire l'objet de connexions non autorisées.

6.B.57 Le rayonnement compromettant n'était pas une menace, grâce à la protection TEMPEST des bâtiments et à l'utilisation de fibres optiques.

6.B.58 Par conséquent, une attaque ne peut être perpétrée que localement, par le réseau :

a) un utilisateur peut tenter d'accéder à un service pour lequel il n'est pas autorisé ;

b) un utilisateur peut se faire passer pour un autre utilisateur (mascarade).

6.B.59 Les utilisateurs autorisés sont considérés comme étant digne de confiance, il n'y a donc pas de risque de mauvaise utilisation du système ou de collusion avec un attaquant.

Politique de sécurité système

6.B.60 Pour l'évaluation d'un système, l'environnement d'exploitation réel est connu et les menaces sur le système peuvent être prévues. Des contre-mesures qui existent (qui pourrait être une combinaison de contre-mesures électroniques, physiques, organisationnelles et liées au personnel) peuvent être prises en compte et les objectifs de sécurité du système peuvent en être élaborés par le commanditaire. Ces informations sont fournies par une politique de sécurité système.

6.B.61 Une organisation a typiquement plusieurs politiques de sécurité. Il existe en général une politique de sécurité à chaque niveau d'une organisation qui dépend des biens relatifs à ce niveau. Par exemple, le système TI d'une organisation aura normalement une politique de sécurité qui spécifira les règles appropriées à la préservation des biens traités par le système et ses composants (par exemple, les données, les matériels, les processus, etc.).

6.B.62 Les politiques de sécurité devraient adapter le niveau de détail à chaque niveau de l'organisation. Par exemple, on n'a pas besoin de spécifier la protection de l'information sensible dans la politique de sécurité organisationnelle initiale mais elle devra être progressivement et itérativement considérée dans les politiques de sécurité de niveau inférieur ainsi que dans la définition de leurs fonctions dédiées à la sécurité (Cf. figure 6.B.2).

6.B.63 La politique de sécurité du système définit les lois, les règles et les procédures qui contrôlent comment l'information sensible et les autres ressources sont gérées à l'intérieur du système. Contrairement à la politique de sécurité technique, elle contient des mesures physiques, organisationnelles et liées au personnel.

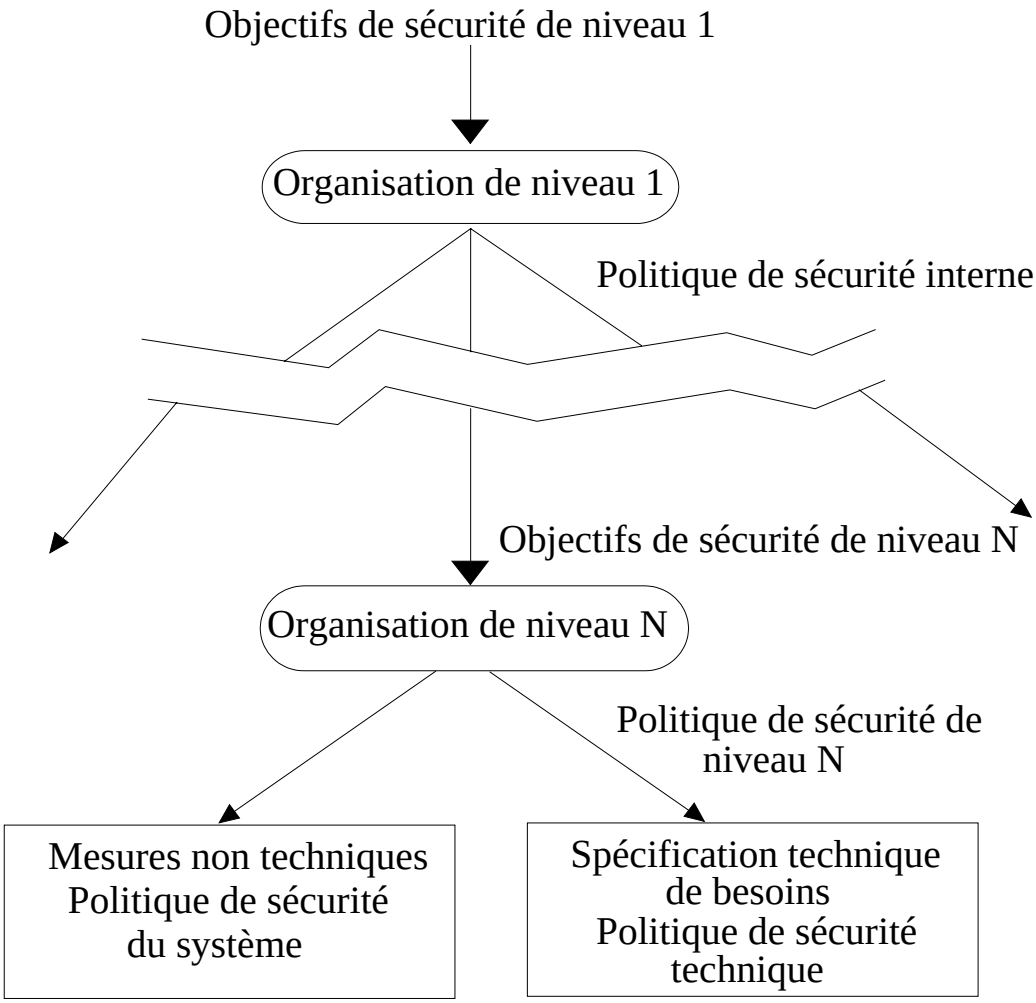


Figure 6.B.2 Elaboration d'une politique de sécurité

6.B.64 La politique de sécurité technique définit les règles de contrôle du traitement des données sensibles et l'utilisation des ressources à l'intérieur même du système.

6.B.65 La politique de sécurité établit vraiment une relation entre les exigences de sécurité définies dans les étapes "menaces" et "objectifs", et les fonctions dédiées à la sécurité définies plus tard dans la cible de sécurité. Du point de vue de l'organisation, l'information déjà contenue dans la politique de sécurité suffit à construire une spécification de réalisation. Cependant, l'information demande à être davantage raffinée avant de pouvoir constituer une spécification des besoins pour la cible d'évaluation. Ce raffinement est l'objectif de la dernière étape dans l'établissement d'une politique de sécurité.

6.B.66 Les objectifs de sécurité et les menaces identifiées suggèrent des règles pour contrôler les multiples utilisateurs de la cible d'évaluation.

6.B.67 Les règles établissent :

a) quelles opérations sont obligatoires, autorisées ou interdites pour chaque bien ;

b) dans quels rôles peuvent, doivent ou ne doivent pas être engagées ces opérations.

6.B.68 Les règles représentent la réponse de l'organisation à l'exigence de sécurité, elles sont le résultat :

a) de l'expérience générale en sécurité ;

b) de doctrines à l'intérieur de l'organisation ;

c) de plans spécialement conçus pour résoudre le problème considéré.

6.B.69 De plus, les principes généraux de sécurité suivants doivent être acceptés :

a) la séparation rôles/utilisateurs, ce qui a pour but de limiter la possibilité d'une attaque résultant de la propagation de droits entre utilisateurs ; cela est particulièrement vrai dans le cas de la suppression de rôles ou d'utilisateurs d'un système ;

b) la facilité d'emploi, qui vise à éviter des erreurs dans l'exploitation de la cible d'évaluation, qui pourraient engendrer des vulnérabilités ;

c) la protection par défaut, qui vise à éviter la nécessité de mesures actives pour maintenir la sécurité ;

d) l'élimination des exceptions, qui vise à rendre le modèle de sécurité plus facile à comprendre et à accepter ;

e) le moindre privilège, qui vise à réduire le risque d'abus, en exigeant que le niveau d'autorisation attribué (à un utilisateur, un rôle, un processus, ...) soit juste suffisant pour l'exécution de sa tâche.

6.B.70 La politique de sécurité achevée doit posséder une logique interne et doit aborder tous les objectifs de sécurité et toutes les menaces.

6.B.71 Les critères ITSEC exigent que les règles de la politique de sécurité soient séparées en deux sous-ensembles :

a) les mesures non techniques, constituées des mesures physiques, organisationnelles ou liées au personnel, établies pour contrôler l'environnement dans lequel la cible d'évaluation agit (par exemple, la politique de sécurité système) ;

b) les mesures techniques, qui constituent les spécifications des besoins de sécurité à partir desquelles des fonctions dédiées à la sécurité peuvent être développées (par exemple, la politique de sécurité technique).

Le système SWAN : politique de sécurité système

6.B.72 Une première formulation de haut niveau de la politique de sécurité système pourrait être résumée par les règles suivantes :

a) un utilisateur peut accéder aux services qui lui sont autorisés ;

b) une personne ne doit pas avoir accès aux services qui lui sont interdits.

6.B.73 Il faut noter que :

a) cette formulation, à travers le concept d'"autorisation", implique un administrateur pour l'attribution et la vérification des autorisations ;

b) l'autorisation, à son tour, introduit un ensemble supplémentaire de ressources, dont l'intégrité est sensible ;

c) cette formulation n'est pas rigoureuse puisqu'elle n'impose aucune obligation à l'utilisateur.

6.B.74 La règle (a) ne concerne que les utilisateurs et ne s'intéresse pas au système, qui n'est pas tenu de fournir un niveau particulier de service, d'après l'hypothèse de départ (pas d'objectifs de disponibilité). Par conséquent, la règle (a) est évidemment une mesure non technique.

6.B.75 Par contre, la règle (b) se réfère au système, qui est censé rendre cette interdiction effective. Il s'agit donc d'une mesure de sécurité technique qui doit être réécrite.

a) le système doit refuser l'accès aux services non autorisés.

6.B.76 Cette formulation de la politique de sécurité est d'un niveau trop élevé, car on ne tient pas encore compte des exigences externes du système. Ces exigences indiquent entre autres que ce système est un réseau qui établit des connexions entre terminaux et systèmes hôtes, comme le permet la politique par contrôle d'accès obligatoire, et que chaque service applicatif est géré localement par un administrateur, sur une base discrétionnaire. Tous ces points sont des ressources sensibles et des devoirs qu'il faut rendre explicites dans une description plus précise de la politique de sécurité. La règle b) peut être reformulée ainsi :

a) (1) le système doit refuser l'accès aux connexions non autorisées ;

b) (2) le système doit refuser l'accès aux systèmes hôtes non autorisés.

6.B.77 Rendre les menaces explicites permet de diviser la règle (1) en deux points :

a) (1.1) le système doit empêcher les intrusions dans les connexions ;

b) (1.2) le système doit refuser l'accès aux connexions non autorisées, selon une politique de contrôle d'accès obligatoire.

6.B.78 Il n'existe aucune règle qui corresponde aux points (1) et (2) pour les terminaux qui sont à la fois passifs et sous surveillance, et qu'on ne considère pas comme être menacés.

6.B.79 On peut maintenant rendre explicites les règles qui définissent les obligations de l'administrateur, en deux règles complémentaires :

a) (3) un administrateur d'applications peut modifier les autorisations (d'utilisation) de services ;

b) (4) le système doit refuser que toute autre personne modifie les autorisations.

6.B.80 Les obligations de l'administrateur réseau (y compris la responsabilité des niveaux de sécurité attribués aux systèmes hôtes) peuvent être explicitées de la même manière.

Modèle formel de politique de sécurité

6.B.81 Les évaluateurs doivent vérifier de manière indépendante la cohérence de la politique de sécurité. Les règles peuvent être amendées sous une forme mathématique pour faciliter leur vérification. Ceci conduit au concept de modèle formel de politique de sécurité, exigé pour une évaluation de niveau E4 et supérieur.

Argumentaire du produit

6.B.82 Un produit peut être utilisé dans différents systèmes et environnements d'exploitation, le véritable environnement d'exploitation d'un produit n'est donc pas connu. La cible de sécurité ne peut que définir la méthode d'utilisation prévue et émettre des hypothèses quant à l'environnement d'exploitation dans lequel le produit devra être utilisé, et sur les menaces à l'encontre desquelles ses fonctions dédiées à la sécurité ont été conçues.

6.B.83 Pour un produit, la cible de sécurité doit contenir une liste d'annonces sur la cible d'évaluation, faites par le commanditaire (généralement le fournisseur du produit), dans le but de fournir à un acheteur potentiel suffisamment d'information pour déterminer si le produit est approprié pour satisfaire certains ou tous ses objectifs de sécurité du système. Ces informations sont fournies sous la forme d'un argumentaire du produit.

6.B.84 Un produit peut être destiné à être utilisé dans différentes configurations. Par exemple, une base de données peut fonctionner sur une machine indépendante ou être utilisée comme base de données répartie dans un environnement réseau. Pour de tels produits, il n'est pas souhaitable ni faisable d'évaluer toutes les configurations, et dans ce cas, les évaluateurs et le commanditaire doivent s'entendre sur la (les) configuration(s) à évaluer. Ceci doit être documenté dans la cible de sécurité

6.B.85 Après avoir réalisé une étude de marché, le fournisseur du produit doit être capable d'affirmer que le produit est en mesure de protéger un bien spécifique (ou un ensemble de biens) qui existe dans un environnement prévu. De plus, le fournisseur doit être capable d'identifier certaines menaces (pertinentes dans l'environnement prévu) que le produit est capable de contrer.

Fonctions dédiées à la sécurité

6.B.86 Les fonctions dédiées à la sécurité (FDS) sont, au plus haut niveau d'abstraction, une déclaration de la fonctionnalité exigée pour satisfaire les objectifs de sécurité. Les FDS doivent fournir un tout inaltérable et incontournable, qui satisfasse pleinement les exigences formulées dans la politique de sécurité.

6.B.87 La première étape de la spécification des FDS est la formulation d'une FDS pour chaque règle individuelle de la politique de sécurité qui établit une relation bijective entre FDS et règles. De telles FDS sont appelées *FDS opérationnelles*, car elles réalisent directement la politique de sécurité. On peut énoncer de nouvelles FDS fournissant des fonctions pour assister les FDS opérationnelles. De telles FDS sont appelées *FDS de soutien*.

6.B.88 Les FDS opérationnelles peuvent être classées selon l'un des quatre types de fonctions suivants :

a) les fonctions de prévention, qui visent à empêcher des attaques potentielles en minimisant les biens ; par exemple, un système peut être débarrassé de ses informations sensibles entre deux sessions utilisateurs.

b) les fonctions de détection, qui ont pour but de détecter les attaques et d'en garder les traces ;

c) les fonctions de cloisonnement, qui visent à contrôler l'accès aux ressources sensibles ; de telles fonctions peuvent bâtir des cloisonnements, appliquer des masques de protection ou empêcher d'accéder à des données transitoires. Les mécanismes cryptographiques sont souvent des fonctions de cloisonnement.

d) des fonctions de rétablissement, qui permettent une reprise sûre de la cible d'évaluation après une panne ou une attaque.

6.B.89 Une fois que toutes les FDS opérationnelles ont été formulées, l'auteur de la cible de sécurité peut déterminer les FDS de soutien nécessaires. De telles FDS doivent assurer que les FDS opérationnelles fonctionnent correctement tout le temps et ne peuvent pas être contournées. Les FDS de soutien sont importantes car elles fournissent une protection pour un sous-ensemble de ressources, i.e. les FDS elles-mêmes. La détermination des FDS de soutien est un processus itératif qui s'achève lorsque toutes les FDS (y compris les FDS de soutien elles-mêmes) sont protégées.

6.B.90 Ce processus itératif est adapté au développement de la cible de sécurité. Toutefois, les ITSEC ne font aucune différence entre FDS de soutien et FDS opérationnelles, mais suggèrent plutôt que toutes les FDS soient classées selon les rubriques génériques suivantes :

a) identification et authentification ;

b) contrôle d'accès ;

c) imputabilité ;

d) audit ;

e) réutilisation d'objets ;

f) fidélité ;

g) fiabilité du service ;

h) échange de données.

6.B.91 Une telle classification des FDS est destinée à faciliter la comparaison entre différentes cibles d'évaluation.

6.B.92 Les classes de fonctionnalité pré-définies forment une partie des ITSEC, si bien qu'on a tendance à utiliser ces rubriques génériques de préférence aux autres.

6.B.93 Une FDS se rapportera souvent à plus d'une rubrique. Dans ce cas, on établira une référence croisée vers les autres rubriques. Si une rubrique générique particulière n'est pas pertinente pour une classe de fonctionnalité, alors elle sera omise.

6.B.94 A cette étape, les FDS doivent être décrites à un niveau de détail adéquat pour montrer leur correspondance avec la politique de sécurité sous-jacente.

Le système SWAN : fonctions dédiées à la sécurité

6.B.95 Pour satisfaire la formulation de la politique de sécurité technique, les développeurs de SWAN ont proposé les fonctions suivantes :

a) Les connexions entre terminaux et systèmes hôtes doivent être chiffrées par des dispositifs "approuvés", placés devant les points d'accès au réseau. Les clefs de chiffrement sont spécifiques aux systèmes d'extrémité. Il est établi que ce choix est efficace contre les intrusions dans les réseaux et est une solution à la règle (1.1).

b) Une fonction qui contrôle l'accès aux systèmes hôtes est installée sur le réseau. Cette fonction réalise une politique de contrôle d'accès obligatoire qui a pour effet d'empêcher l'ouverture de circuits virtuels entre un terminal et un système hôte qui ne sont pas au même niveau de sécurité. Ce choix est une solution à la règle (1.2).

c) Les fonctions de contrôle d'accès discrétionnaire sont maintenues telles qu'elles étaient définies dans l'ancienne solution dédiée à chaque serveur. Cette décision imposée par des exigences externes est représentative de contraintes spécifiques au système et à l'environnement ; c'est une solution à la règle (2).

6.B.96 Le développeur propose une quatrième fonction de sécurité (Cf. l'exemple de SWAN dans le chapitre 5 de l'ITSEM) pour réaliser l'authentification des utilisateurs qui demandent l'accès au réseau. Cette fonction est-elle superflue, si l'on considère que trois fonctions seulement semblent couvrir la politique de sécurité ? Il est évident que le contrôle d'accès réseau (fonction 2) implique une authentification des terminaux. Le contrôle d'accès n'est pas réalisable sans lui associer l'authentification. Auquel cas, le contrôle d'accès doit-il être explicite ?

6.B.97 Si en général la réponse est *non*, sa formulation explicite peut être retardée jusqu'au raffinement du contrôle d'accès. Dans le cas présent, le développeur a choisi d'utiliser une authentification équivalente des utilisateurs plutôt qu'une authentification des terminaux.

6.B.98 Une présentation complète des FDS de SWAN requerrait l'analyse des fonctions de soutien nécessaires pour garantir l'exécution correcte des quatre fonctions opérationnelles décrites. Cette présentation contiendrait les mesures adoptées pour vérifier ces fonctions, maintenir les éléments secrets, ou contourner les contrôles réseau. Ces mesures sont justifiées par la protection des ressources sensibles récemment introduites dans la définition du système. Tous ces problèmes sont présentés dans le chapitre 5 de l'ITSEM comme des problèmes de réalisation, mais doivent aussi être pris en compte dans la cible de sécurité.

Mécanismes de sécurité requis

6.B.99 Une cible de sécurité peut de manière optionnelle prescrire ou revendiquer l'utilisation de mécanismes de sécurité particuliers, i.e. des dispositifs, des algorithmes ou des procédures qui devraient être utilisées pour réaliser certaines FDS. De tels mécanismes contiennent vraisemblablement :

a) des algorithmes tels que des algorithmes de chiffrement de données, des algorithmes de hachage, des codes correcteurs d'erreur et des algorithmes de génération de mots de passe ;

b) des mécanismes d'identification et d'authentification tels que les dispositifs biométriques (reconnaissance vocale, empreintes digitales) et dispositifs personnels d'identification (PID).

6.B.100 De tels mécanismes peuvent être rendus obligatoires par l'analyse réalisée pendant la spécification des besoins de sécurité.

6.B.101 En règle générale, l'auteur de la cible de sécurité devrait éviter des sur-spécifications de mécanismes de sécurité qui rendraient obligatoires à la fois les objectifs de sécurité et les mesures adoptées pour les réaliser.

6.B.102 Jusqu'à présent la cible de sécurité a spécifié les FDS de façon abstraite sans faire référence aux mécanismes les réalisant. En pratique, chaque FDS est réalisée par un ou plusieurs mécanismes, chacun d'eux pouvant traiter plusieurs FDS.

6.B.103 Lors de la spécification des mécanismes requis, l'auteur doit décider s'ils relèvent de la sécurité et donc, s'ils ont leur place dans la cible de sécurité.

6.B.104 En principe, la spécification des mécanismes de sécurité devrait seulement se limiter à couvrir les besoins de sécurité. Ces besoins peuvent suggérer l'utilisation d'une technique particulière, un algorithme, un composant ou une méthode de développement. Elles peuvent même couvrir l'utilisation d'un produit ou d'un développeur particulier.

6.B.105 On considère que les attributs qui ne sont pas spécifiés dans la cible de sécurité font implicitement partie du processus de réalisation et reviennent au développeur. De tels choix ont à être justifiés dans les fournitures destinées à l'évaluation.

Le système SWAN : mécanismes de sécurité requis

6.B.106 L'exemple du SWAN ne fait pas mention de mécanismes de sécurité requis pour l'installation du système. Néanmoins, on peut imaginer que le développeur souhaite réutiliser les mécanismes d'authentification par mot de passe déjà présents dans le serveur.

Cotation annoncée de la résistance minimum des mécanismes

6.B.107 Un mécanisme est la logique ou l'algorithme réalisant une fonction particulière de sécurité dédiée ou touchant à la sécurité.

6.B.108 Certains mécanismes présentent une faiblesse sous-jacente dans le fait qu'un attaquant peut en venir à bout en utilisant des ressources, un équipement spécial ou profitant d'une opportunité. Un système d'authentification qui pourrait être mis en échec par l'essai successif de tous les mots de passe en est un exemple.

6.B.109 De tels mécanismes peuvent être cotés comme élémentaires, moyens ou élevés en fonction du niveau des attaques auxquelles ils peuvent résister (voir l'annexe 6.C pour plus d'informations).

6.B.110 La cible de sécurité doit annoncer la cotation de la résistance du mécanisme critique le plus faible de la cible d'évaluation.

Le système SWAN : cotation annoncée de la résistance minimum des mécanismes

6.B.111 La résistance minimum des mécanismes demandée pour le système SWAN pris dans sa totalité est *moyenne*.

6.B.112 Afin d'atteindre cette exigence pour le système, le développeur a décrit la résistance individuelle des mécanismes suivants :

a) pour le mécanisme qui réalise la contre-mesure 1 (CM1) qui authentifie les utilisateurs qui se connectent au réseau, la résistance annoncée du mécanisme est *élémentaire* ;

b) pour le mécanisme qui réalise la contre-mesure 2 (CM2) qui fournit le contrôle d'accès, la résistance annoncée du mécanisme est *élevée* ;

c) pour le mécanisme qui réalise la contre-mesure 3 (CM3) qui chiffre les données sur la liaison entre les terminaux et les systèmes hôtes, un mécanisme de résistance *moyenne* approuvé par l'autorité nationale est utilisée ;

d) pour le mécanisme qui réalise la contre-mesure 4 (CM4) qui authentifie les utilisateurs qui se connectent à un système hôte, la résistance annoncée est *moyenne*.

6.B.113 Pour justifier ces choix, le développeur affirme que seul le mécanisme de chiffrement est critique dans la cible de sécurité. Ce raisonnement est correct car même si le mécanisme de contrôle d'accès défaille, l'attaquant a seulement accès aux données chiffrées et est incapable de violer les objectifs de sécurité.

6.B.114 Une analyse (non présentée dans le chapitre 5 de l'ITSEM) a été réalisée et a fourni les résultats suivants :

a) les mécanismes de chiffrement ont été estimés par l'autorité nationale qui a conclu à une résistance *moyenne ;*

b) les mots de passe générés automatiquement sont formés de 8 caractères et ont une période de validité de 60 jours au plus. Il n'y a pas de restriction sur le nombre de présentation de mots de passe invalides ; les services d'authentification réseau et applicatifs ont été coté au niveau *élémentaire* ;

c) la gestion de réseau ou la collusion avec l'administrateur réseau ne sont pas pris en compte ici ; sans considérer l'authentification, le strict contrôle d'accès réseau a été jugé *élevé* en l'absence de menaces autres que celle liées à la surveillance du réseau.

Le niveau d'évaluation

Le choix d'un niveau d'évaluation

6.B.115 La cible de sécurité doit spécifier un niveau d'évaluation visé pour l'évaluation de la cible d'évaluation. Celui-ci doit être un parmi E1, E2, E3, E4, E5 ou E6.

6.B.116 Le choix d'un niveau d'évaluation est un compromis entre ce qui est souhaité (i.e. la plus grande assurance) et ce qui est possible en tenant compte des coûts. Les coûts de l'évaluation ne sont pas les seuls à devoir être pris en compte soigneusement mais d'autres coûts tels que ceux liés à la production et à la livraison des fournitures nécessaires doivent également l'être.

6.B.117 Les figures 6.B.7 et 6.B.8 résument les conséquences du niveau d'évaluation sur le contenu d'une cible de sécurité.

Informations exigées

6.B.118 Les niveaux d'évaluations se différencient par la granularité des informations de conception exigées pour l'évaluation comme indiqué dans le tableau suivant :

Figure 6.B.3 Niveau et information

Niveau d'évaluation	Informations requises
E1	conception générale
E2	conception générale et conception détaillée
E3 et suivants	conception générale, conception détaillée, code source et schémas descriptifs des matériels

Style de spécification

6.B.119 Les différents niveaux d'évaluation exigent différents niveaux de spécification comme précisé dans le tableau suivant :

Figure 6.B.4 Niveau et style

Niveau d'évaluation	Style de spécification
E1, E2, E3	documentation informelle
E4, E5	modèle formel de la politique de sécurité sous-jacente, spécifications semi-formelles des fonctions dédiées à la sécurité et description semi-formelle de l'architecture et de la conception détaillée
E6	modèle formel de la politique de sécurité sous-jacente, spécifications formelles des fonctions dédiées à la sécurité, description formelle de l'architecture et description semi-formelle de la conception détaillée

Rigueur de la spécification

6.B.120 La rigueur du contenu, de la présentation et des éléments de preuve dépend aussi du niveau d'évaluation visé comme l'indiquent les transitions entre les verbes *présenter*, *décrire* et *expliquer*. Les exigences pour chaque niveau d'évaluation sont résumés dans la figure 6.B.5.

Figure 6.B.5 Rigueur de la spécification

Exigences pour les éléments de preuve[1]	Niveau d'évaluation visé					
	E1	E2	E3	E4	E5	E6
	présenter		*décrire*		*expliquer*	
éléments pertinents fournis	✔	✔	✔	✔	✔	✔
caractéristiques pertinentes énumérés			✔	✔	✔	✔
justifications données					✔	✔

[1] NdT : la traduction ITSEC 0.12 a été reprise.

6.B.121 Par exemple, au niveau E1 et E2, une cible de sécurité pourrait décrire ainsi un processus de connexion :

> La <cible d'évaluation> doit identifier et authentifier les utilisateurs autorisés en vérifiant la validité de leur dispositif personnel d'identification, de leur identifiant et de leur mot de passe ainsi que la cohérence entre ces informations. L'utilisateur a droit à trois essais pour réussir sa connexion. Si le nombre de tentatives excède trois, l'échec est enregistré et son identifiant est invalidé.

6.B.122 Aux niveaux E3 et E4, le processus doit être décrit plus précisément en énumérant les caractéristiques du processus de connexion. La cible de sécurité pourrait inclure les déclarations suivantes :

> La <cible d'évaluation> devra identifier et authentifier les utilisateurs autorisés en contrôlant la validité du PID, de l'identifiant et du mot de passe. Le système devra vérifier que :
>
> a) l'identifiant saisi au clavier correspond à celui qui est détenu sous forme informatique par le PID ;
>
> b) l'identifiant est enregistré dans le fichier des utilisateurs autorisés ;
>
> c) le mot de passe est valide pour cet identifiant.
>
> Si le nombre de tentatives excède trois, le système devra :
>
> a) écrire un message d'audit identifiant le type d'incident (i.e. échec de la connexion), l'horodatage de l'incident, l'identification du terminal et le nom de l'utilisateur.

b) verrouiller l'utilisateur hors du système en invalidant l'entrée correspondante dans le fichier des utilisateurs autorisés.

6.B.123 Au niveau E5 et E6, des explications fournissant une justification à la fonctionnalité spécifiée sont exigées. La cible de sécurité pourrait inclure des déclarations telles que celles-ci :

a) L'audit des tentatives de connexion qui ont échoué prévient l'officier de sécurité qu'un terminal particulier, un compte utilisateur spécifique ou le système dans sa globalité est soumis à une attaque.

b) l'entrée de l'utilisateur dans le fichier des utilisateurs autorisés est désactivée pour interdire l'accès au système à l'utilisateur correspondant jusqu'à ce que l'officier de sécurité l'y autorise (éventuellement) à nouveau.

Utilisation d'outils

6.B.124 Les différents niveaux d'évaluation exigent l'utilisation d'outils particuliers tels que décrits dans le tableau suivant :

Figure 6.B.6 Niveau et outils

Niveau d'évaluation	Outils requis
E1	aucun
E2 et suivants	outils de tests
E3 et suivants	langages de programmation parfaitement définis
E4 et suivants	outils de développement, outil de gestion de configuration
E6	outils d'analyse de code

Le système SWAN : niveau d'évaluation

6.B.125 On a choisi le niveau de confiance E3 qui fournit une assurance adéquate et accessible au vu des contraintes financières et des délais.

Figure 6.B.7 Cible de sécurité pour l'évaluation d'un produit

			E1	E2	E3	E4	E5	E6
1.	Introduction							
	1.1	Cotation minimum annoncée pour la RdM {2.25}	❍	❍	❍	❍	❍	❍
	1.2	Niveau d'évaluation visé {2.26}	❍	❍	❍	❍	❍	❍
2.	Argumentaire du produit {2.16-2.17}							
	2.1	Objectifs de sécurité	❍	❍	❍	❍	❍	❍
	2.2	Méthode d'utilisation prévue {2.17}	❍	❍	❍	❍	❍	❍
	2.3	Environnement prévu {2.17}	❍	❍	❍	❍	❍	❍
	2.4	Menaces supposées {2.17}	❍	❍	❍	❍	❍	❍
3.	Modèle de politique de sécurité {2.81-2.83}					●	●	●
4.	Spécification des fonctions dédiées à la sécurité {2.18-2.24}		❍	❍	❍	◗	◗	●
		[Déf. des fonctions dédiées à la sécurité]	❍	❍	❍	◗	◗	●
		[Déf. des mécanismes de sécurité requis (optionnelle)]	❍	❍	❍	◗	◗	●
	4.1	Identification et authentification {2.34-2.36}	❍	❍	❍	◗	◗	●
	4.2	Contrôle d'accès {2.37-2.39}	❍	❍	❍	◗	◗	●
	4.3	Imputabilité {2.40-2.42}	❍	❍	❍	◗	◗	●
	4.4	Audit {2.43-2.45}	❍	❍	❍	◗	◗	●
	4.5	Réutilisation d'objet {2.46-2.48}	❍	❍	❍	◗	◗	●
	4.6	Fidélité {2.49-2.51}	❍	❍	❍	◗	◗	●
	4.7	Fiabilité de service {2.52-2.54}	❍	❍	❍	◗	◗	●
	4.8	Échange de données {2.55-2.58}	❍	❍	❍	◗	◗	●
etc.								

Légende concernant le style de spécification : ❍ Informel ; ◗ Semiformel & informel ; ● Formel & informel

Figure 6.B.8 Cible de sécurité pour l'évaluation d'un système

		E1	E2	E3	E4	E5	E6
1.	Introduction						
1.1	Cotation minimum annoncée de la RdM {2.25}	❍	❍	❍	❍	❍	❍
1.2	Niveau d'évaluation visé {2.26}	❍	❍	❍	❍	❍	❍
2.	Politique de sécurité du système {2.9-2.15}						
2.1	Objectifs de sécurité {2.9}	❍	❍	❍	❍	❍	❍
2.2	Description de l'environnement d'exploitation {2.9}	❍	❍	❍	❍	❍	❍
2.3	Menaces réelles {2.9}	❍	❍	❍	❍	❍	❍
3.	Modèle de politique de sécurité {2.81-2.83}				●	●	●
4.	Spécification des fonctions dédiées à la sécurité {2.18-2.24}	❍	❍	❍	◗	◗	●
	[Déf. des fonctions dédiées à la sécurité]	❍	❍	❍	◗	◗	●
	[Déf. des mécanismes de sécurité requis (optionnelle)]	❍	❍	❍	◗	◗	●
4.1	Identification et authentification {2.34-2.36}	❍	❍	❍	◗	◗	●
4.2	Contrôle d'accès {2.37-2.39}	❍	❍	❍	◗	◗	●
4.3	Imputabilité {2.40-2.42}	❍	❍	❍	◗	◗	●
4.4	Audit {2.43-2.45}	❍	❍	❍	◗	◗	●
4.5	Réutilisation d'objets {2.46-2.48}	❍	❍	❍	◗	◗	●
4.6	Fidélité {2.49-2.51}	❍	❍	❍	◗	◗	●
4.7	Fiabilité de service {2.52-2.54}	❍	❍	❍	◗	◗	●
4.8	Échange de données {2.55-2.58}	❍	❍	❍	◗	◗	●
etc.							

Légende concernant le style de spécification : ❍ Informel ; ◗ Semiformel & informel ; ● Formel & informel

Annexe 6.C Efficacité

Introduction

6.C.1 Cette annexe décrit l'application des critères ITSEC dans le domaine de l'efficacité.

Mécanismes

Classification des mécanismes

6.C.2 Cette section décrit les différents types de mécanismes qui peuvent être utilisés dans une cible d'évaluation.

6.C.3 Un mécanisme de sécurité est défini dans les critères ITSEC au paragraphe 6.46 comme la logique ou l'algorithme qui réalise par matériel ou logiciel une fonction particulière dédiée ou touchant à la sécurité. Un mécanisme critique est défini dans les critères ITSEC au paragraphe 6.48 comme un mécanisme interne d'une cible d'évaluation dont la défaillance créerait une faiblesse dans la sécurité.

6.C.4 Un *mécanisme de type A* est un mécanisme de sécurité qui posséde, dans ses algorithmes, principes ou propriétés, une vulnérabilité potentielle en raison de laquelle ce mécanisme peut être mis en échec par une attaque directe avec des ressources, de la compétence et des opportunités suffisantes. Un exemple d'un mécanisme de type A est un programme d'authentification qui utilise un mot de passe : si le mot de passe peut être deviné par l'essai de tous les mots de passe possibles en série, le mécanisme d'authentification est de type A. Les mécanismes de type A font souvent appel à un "secret" comme un mot de passe ou une clef cryptographique.

6.C.5 Tous les mécanismes de type A d'une cible d'évaluation ont une résistance qui correspond au niveau de ressources, de compétence et d'opportunité nécessaire pour compromettre la sécurité en attaquant directement ce mécanisme.

6.C.6 Pour l'estimation de la résistance d'un mécanisme, le contexte dans lequel le mécanisme est utilisé devrait être pris en considération. Voir la sous-section *Exemple* ci-dessous.

6.C.7 Un *mécanisme de type B* est un mécanisme de sécurité qui, s'il est parfaitement conçu et réalisé, n'aura aucune faiblesse. Un mécanisme de type B peut être considéré comme toujours résistant à une attaque directe sans considération de niveau de ressources, de compétence ou d'opportunité. Un exemple possible de mécanisme de type B serait un contrôle d'accès basé sur des listes de contrôle d'accès : s'il est parfaitement conçu et réalisé, ce mécanisme de type B ne peut pas être mis en échec par une attaque directe. Cependant, ces mécanismes de type B peuvent être mis en échec par des attaques indirectes qui font l'objet d'autres analyses d'efficacité.

6.C.8 La cible de sécurité pour une cible d'évaluation devrait spécifier la résistance minimum des mécanismes, i.e. la résistance du mécanisme critique de type A le plus faible de la cible d'évaluation. L'analyse de la résistance des mécanismes effectuée par le développeur pourrait :

a) identifier les mécanismes critiques et expliquer pourquoi les autres mécanismes ne sont pas critiques ;

b) énoncer et confirmer la résistance de chaque mécanisme critique de type A ;

c) confirmer que les mécanismes critiques de type B n'ont pas de faiblesses (peut-être en faisant référence à d'autres analyses d'efficacité).

Exemple

6.C.9 Un mécanisme de sécurité est la logique ou l'algorithme qui réalise par logiciel ou matériel une fonction dédiée ou touchant à la sécurité particulière. Par exemple, un algorithme de mot de passe *A* complexe pourrait être dérivé d'un algorithme de mot de passe B simple, renforcé par le principe *C* de limitation du nombre d'essais après échec d'authentification : un développeur pourrait considérer cet algorithme *A* comme réalisé par un seul mécanisme de sécurité M_A, tandis qu'un autre développeur peut choisir de considérer le même algorithme *A* comme réalisé par deux mécanismes M_B qui réalise l'algorithme *B* et M_C qui réalise le principe *C*. Ainsi, si la conception existante n'utilise que l'algorithme *B* et si les développeurs choisissent tous les deux de le renforcer en utilisant l'algorithme *A* :

a) le premier développeur considérera ce plan d'action comme le renforcement du mécanisme ;

b) le second développeur considérera le même plan d'action comme l'utilisation d'un autre mécanisme.

6.C.10 Comme les deux plans d'actions sont en pratique identiques, les cas des paragraphes a) et b) ci-dessus sont équivalents. La figure 6.C.1 illustre les deux situations.

6.C.11 Dans la figure, les mécanismes A et B sont tous les deux de type A parce qu'ils peuvent être mis en échec par une attaque directe (par exemple, essais répétés de mots de passe). Le mécanisme A et le mécanisme B dans le contexte du mécanisme C ont une résistance identique. Le mécanisme A tire une partie de sa résistance du fait qu'il comprend une limitation du nombre d'essais. Le mécanisme B ne comporte pas cette limitation mais il doit être évalué en prenant en compte son contexte. Par conséquent, le fait que le mécanisme C limite les essais augmente la résistance de la combinaison des mécanismes B et C.

Les critères d'efficacité

Efficacité et conformité

6.C.12 En général, la répartition du travail entre conformité et efficacité dépend de la cible de sécurité. En effet, la conformité s'applique à la fonctionnalité et est mesurée par rapport à ce qui est spécifié dans la cible de sécurité alors que l'efficacité est relative à l'absence de vulnérabilités exploitables. Plus il y a de détails dans la cible de sécurité, plus grand est l'effort d'évaluation destiné à l'estimation de la conformité.

6.C.13 Par exemple, une cible de sécurité pourrait exiger qu'une fonction d'identification et d'authentification soit réalisée avec une résistance de mécanisme élevée, mais ne pas spécifier le mécanisme. Une réalisation qui autoriserait des utilisateurs à avoir des mots de passe de deux caractères serait rejetée car inefficace. Si la cible de sécurité interdisait des mots de passe de deux caractères, la même réalisation aurait échoué pour des raisons de conformité.

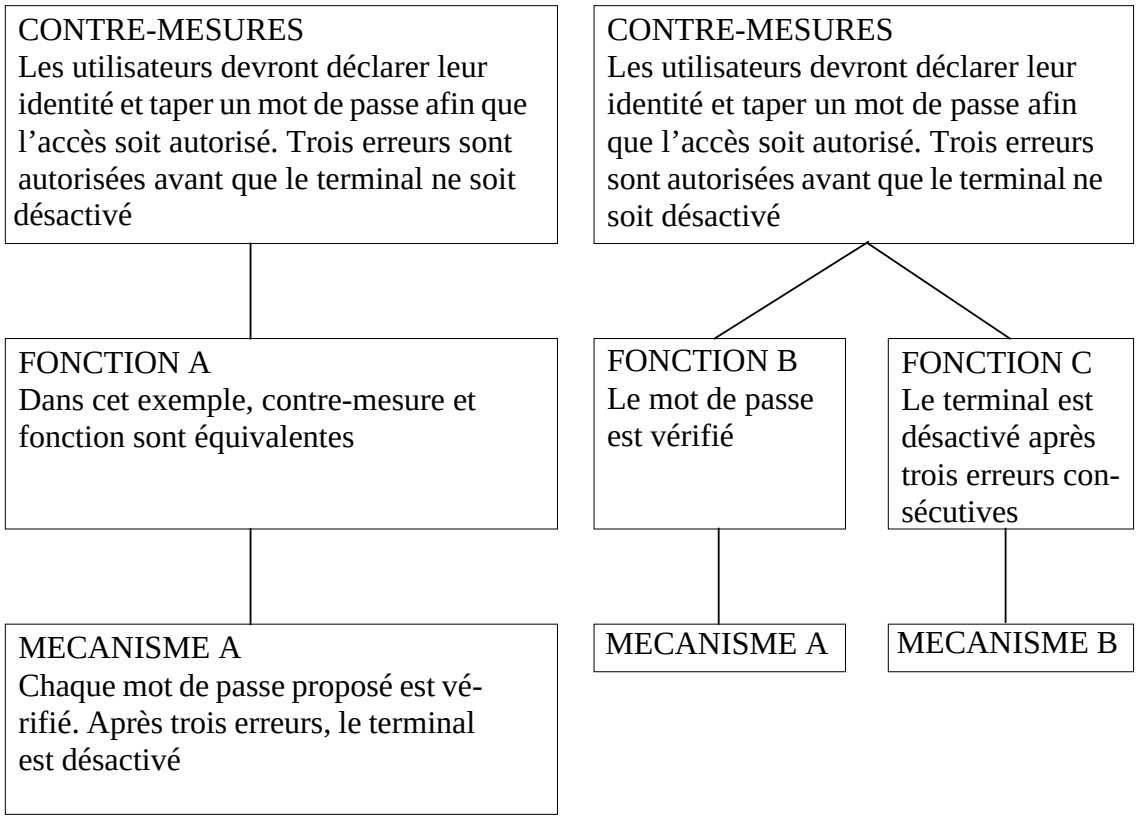


Figure 6.C.1 Deux façons de traiter les mécanismes

Aspects de l'efficacité

6.C.14 Cette sous-section considère les relations entre critères d'efficacité.

6.C.15 Il est constructif de considérer les critères d'efficacité du point de vue du développeur. Le développeur devrait effectuer une estimation de risque pour déterminer les fonctions dédiées à la sécurité nécessaire, en se fondant sur les éléments suivants :

a) une définition générale de la fonctionnalité (ne touchant pas à la sécurité) requise de la cible d'évaluation ;

b) les menaces envers la cible d'évaluation et/ou les objectifs de sécurité de la cible d'évaluation ;

c) les biens à protéger par la cible d'évaluation (les biens peuvent être des informations ou du logiciel dont la confidentialité, l'intégrité et la disponibilité doivent être protégées).

6.C.16 En choisissant ses fonctions dédiées à la sécurité, le développeur devrait décider si elles sont :

a) pertinentes, dans le sens où elles devraient contrer la ou les menaces ;

b) capable de coopérer pour former un ensemble intégré et efficace (i.e. agir en cohésion), dans le cas où plus d'une fonction dédiée à la sécurité a été choisie.

6.C.17 Une illustration simple et schématique de ce processus est fournie figure 6.C.2. Cette figure (ainsi que les figures 6.C.3 et 6.C.4) représentent :

a) les biens par le symbole "ECU" ;

b) les menaces par des "clous" dont la longueur est "proportionnelle" au niveau de compétence, d'opportunité et de ressource dont dispose l'attaquant ;

c) les contre-mesures (par exemple, les fonctions dédiées à la sécurité) par un "mur" dont l'épaisseur est "proportionnelle" à la résistance du mécanisme de type A qui le réalise (i.e., la capacité des contre-mesures à protéger d'une attaque directe).

6.C.18 Plus le "clou" est long, plus la gravité de la menace est grande ; plus le mur est épais, plus la capacité de la contre-mesure à défendre les biens contre cette menace est grande. En effet, la cible d'évaluation est jugée sûre si les biens sont complètement entourés par un mur qui a une épaisseur minimum supérieure ou égale à la longueur de tout clou.

6.C.19 La figure 6.C.2 illustre le cas où les fonctions dédiées à la sécurité choisies sont insuffisantes pour contrer la menace, bien que leurs mécanismes soient de résistance suffisante. La figure illustre l'architecture d'un système d'exploitation sécurisé (par exemple F-B2) pour lequel le développeur a négligé d'introduire les mécanismes nécessaires pour protéger des altérations et interférences externes les fonctions dédiées à la sécurité traditionnelles (par exemple, identification et authentification, contrôle d'accès, etc.). En effet, à cette étape de l'estimation des vulnérabilités, le développeur pourrait affirmer que sa solution, dans cet état :

a) n'est pas pertinente car elle ne contrera pas la menace ;

b) n'assure pas la cohésion car elle ne forme pas un ensemble intégré.

6.C.20 Ces défauts sont corrigés dans la figure 6.C.3, qui montre l'introduction d'un deuxième lot de contre-mesures qui ont pour objectif de protéger le premier lot contre des altérations ou des interférences externes.

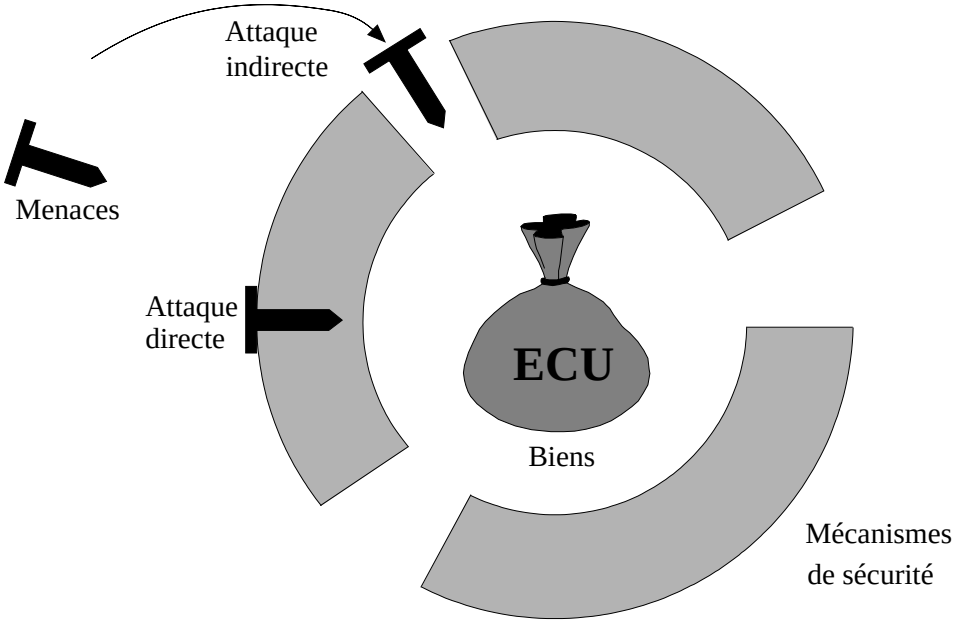


Figure 6.C.2 L'échec de la pertinence et de la cohésion

6.C.21 Cette figure indique également l'épaisseur des "murs" de contre-mesures nécessaires pour satisfaire aux définitions ITSEC de la résistance des mécanismes (RdM) : *élémentaire, moyenne* et *élevée.* Les mécanismes de protection sont représentés comme ayant une cotation *élevée* et les contre-mesures initiales comme ayant une cotation *moyenne*. Si la RdM minimum (RdM_{min}) est *moyenne*, alors cette figure indique que la cible d'évaluation devrait satisfaire aux critères de pertinence, de cohésion et de résistance des mécanismes :

a) l'épaisseur minimum du "mur" est moyenne, et ainsi satisfait à l'exigence de RdM ;

b) le "mur" entoure complètement les biens et il n'y a pas d'ouverture, par conséquent, les contre-mesures contrent la menace et les critères de pertinence et de cohésion sont satisfaits.

6.C.22 A chaque étape du développement, le développeur devrait répéter son estimation des vulnérabilités. En effet, du point de vue de l'évaluation, il devrait le faire jusqu'à ce que toutes les informations citées dans la figure 4 des critères ITSEC aient été considérées pour le niveau d'évaluation considéré.

6.C.23 Dans la figure 6.C.4(a), une vulnérabilité est représentée comme une "réduction de l'épaisseur du mur des contre-mesures", i.e. une épaisseur inférieure à celle exigée par la RdM_{min}. Dans ce cas, la cotation de la résistance des mécanismes de la cible d'évaluation est celle du mécanisme critique qui a la plus faible cotation.

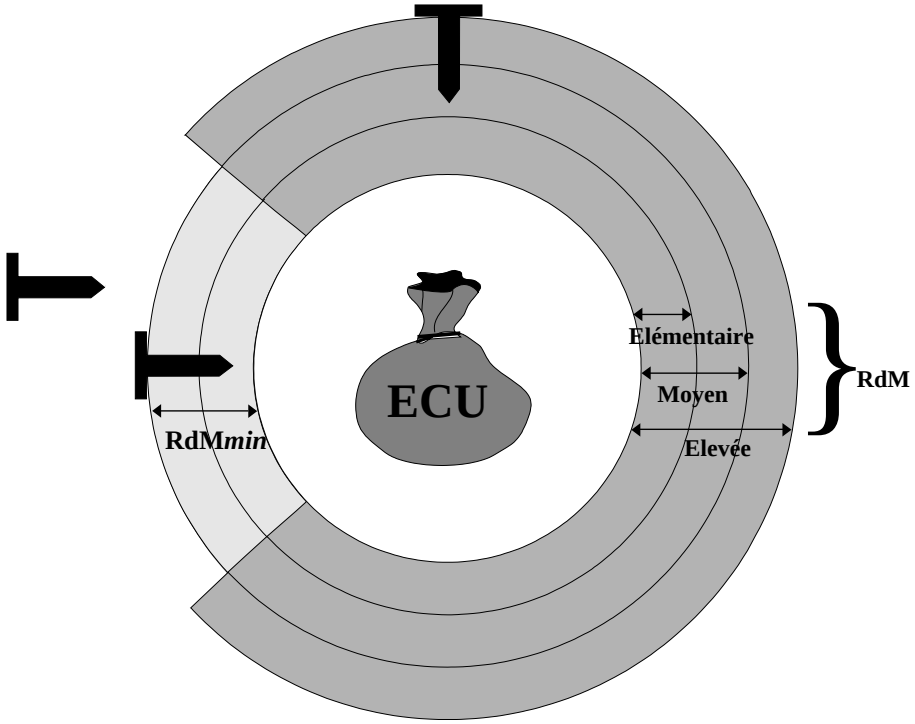


Figure 6.C.3 Une cible d'évaluation sûre

6.C.24 Conformément aux critères ITSEC, il y a quatre directions dans lesquelles le développeur peut modifier ou faire évoluer sa conception afin de contrer cette vulnérabilité :

a) le développeur est libre de considérer la vulnérabilité comme un défaut des algorithmes, principes et propriétés sous-jacents des mécanismes chargés de satisfaire la RdM_{min}. Dans ce cas, le recours du développeur consiste à modifier les algorithmes, principes et propriétés existants (ou à adopter de nouveaux algorithmes, principes et propriétés) qui satisfont effectivement la RdM_{min} exigée. Si le développeur opte pour ce plan d'action, le résultat sera tel que décrit en figure 6.C.4(b).

b) Sinon, comme indiqué dans les critères ITSEC, au paragraphe 3.27 (premier point) du critère Estimation de la **vulnérabilité de construction**, le développeur peut introduire un ou des mécanismes de sécurité supplémentaires internes à la cible d'évaluation. Si le développeur opte pour ce plan d'action, le résultat sera tel que décrit en figure 6.C.4(b). En effet, ce plan d'action est synonyme du premier.

c) Comme indiqué dans les critères ITSEC au second point du paragraphe 3.27 du critère Estimation de la vulnérabilité de la construction (comme pour le critère **vulnérabilité en exploitation**), le développeur peut exiger l'introduction d'une contre-mesure externe. Pour ce plan d'action, le résultat sera tel que décrit en figure 6.C.4(c). Si ce plan est suivi, la contre-mesure devrait être documentée dans la cible de sécurité.

d) Finalement, selon le critère Facilité d'emploi, le développeur pourrait introduire une combinaison de mesures internes et externes qui, bien qu'elles ne permettent pas de contrer directment la vulnérabilité (i.e. en augmentant l'épaisseur du mur), permettent de porter à l'attention d'un utilisateur ou d'un administrateur toute tentative d'exploitation de la vulnérabilité. Ce plan d'action est décrit en figure 6.C.4(d) et serait, par exemple, le cas où l'utilisation de canaux cachés qui ne peuvent pas être supprimés est surveillée par un système d'exploitation sécurisé.

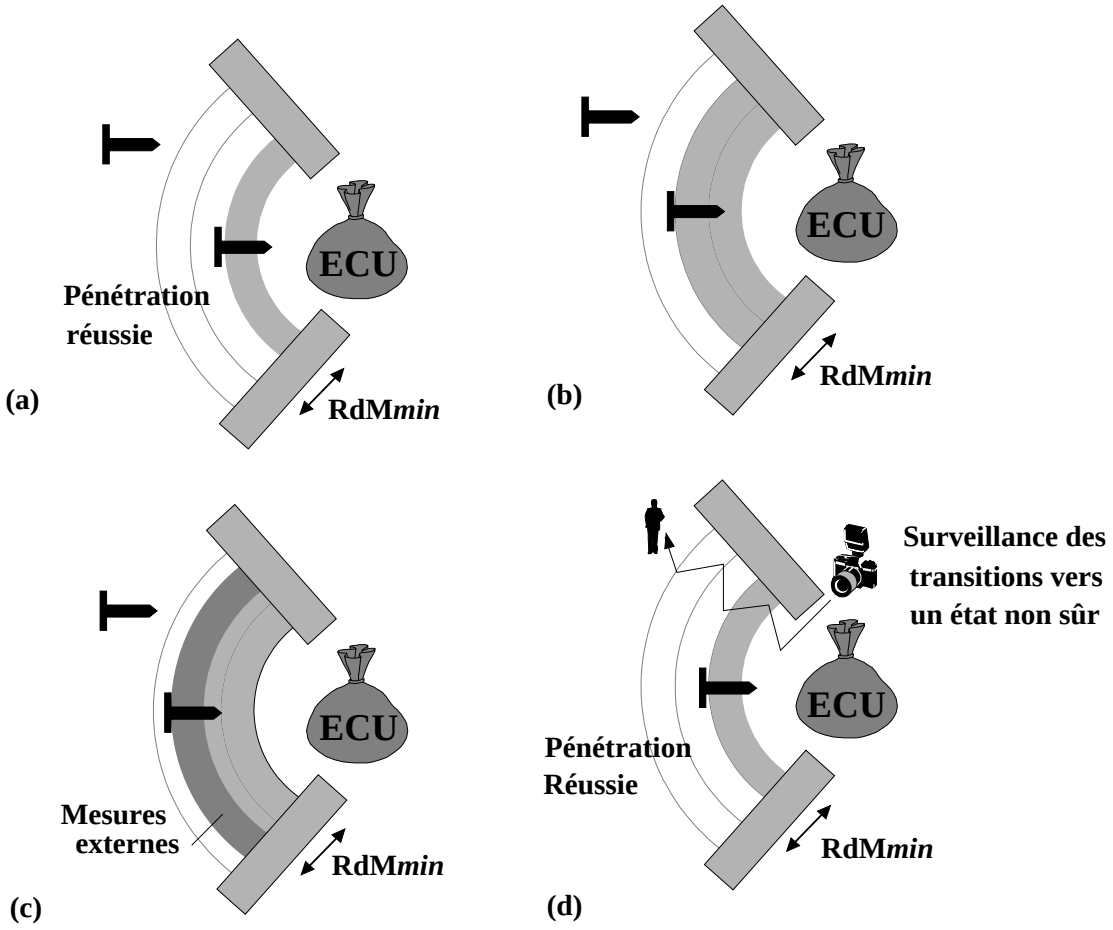


Figure 6.C.4 Résorber des vulnérabilités de sécurité

6.C.25 Une fois que le développeur a choisi comment il allait contrer les vulnérabilités identifiées précédemment, l'application du critère de cohésion de la fonctionnalité vérifiera que la solution résout bien le problème de vulnérabilité (tel qu'il est identifié à ce niveau de conception) et n'introduit aucune nouvelle vulnérabilité. Si une nouvelle vulnérabilité venait à être découverte, alors le développeur devrait revenir sur ses pas, en choisissant des solutions à base de contre-mesures externes et internes différentes, jusqu'à ce que le critère de cohésion de la fonctionnalité soit enfin satisfait.

6.C.26 Il faudrait noter que lorsqu'une vulnérabilité est découverte, il sera parfois possible de la caractériser de plusieurs manières : par exemple, il peut être difficile de décider s'il s'agit d'un problème de pertinence ou de cohésion. En pratique, ce n'est pas un problème. Il est plus important d'avoir la confiance que toutes les vulnérabilités ont été découvertes que de pouvoir facilement faire la distinction entre les différents types de vulnérabilités.

6.C.27 En résumé, les erreurs d'efficacité peuvent être de deux types :

a) des erreurs dans le contenu, la présentation et les éléments de preuve pour une fourniture particulière relative à l'efficacité. Ce type d'erreur correspondra à un aspect particulier de l'efficacité ;

b) des vulnérabilités découvertes au cours des tests de pénétration. Il peut être plus difficile d'assigner à ce type de vulnérabilité un aspect particulier de l'efficacité.

Estimation de la résistance des mécanismes

6.C.28 D'après les critères ITSEC (paragraphe 3.6 à 3.8) la signification de cotations de la résistance des mécanismes est la suivante :

a) pour que la résistance minimum d'un mécanisme critique soit cotée *élémentaire*, il doit être manifeste qu'il fournit une protection contre une subversion accidentelle aléatoire, bien qu'il soit susceptible d'être mis en échec par des agresseurs compétents.

b) pour que la résistance minimum d'un mécanisme critique soit cotée *moyenne*, il doit être manifeste qu'il fournit une protection contre des agresseurs dont les opportunités ou les ressources sont limitées.

c) pour que la résistance minimum d'un mécanisme critique soit cotée *élevée*, il doit être manifeste qu'il ne pourra être mis en échec que par des agresseurs disposant d'un haut degré de compétence, d'opportunité et de ressources, une attaque réussie étant jugée normalement au delà du réalisable.

6.C.29 Ces définitions sont informelles et destinées à être significatives pour les utilisateurs d'une cible d'évaluation. Cette sous-section donne des indications sur des moyens de mesure plus objectifs.

6.C.30 Puisque la résistance des mécanismes est relative à la compétence, aux opportunités et aux ressources, il est nécessaire de développer la signification de ces termes :

a) La *compétence* représente la connaissance nécessaire aux personnes pour pouvoir attaquer une cible d'évaluation. Un *profane* est quelqu'un sans compétence particulière ; une personne *compétente* est quelqu'un qui connait bien les fonctionnements internes de la cible d'évaluation, et un *expert* est quelqu'un connait bien les principes et algorithmes sous-jacents utilisés dans la cible d'évaluation.

b) Les *ressources* représentent les ressources qu'un attaquant doit employer pour attaquer avec succès la cible d'évaluation. Les évaluateurs s'intéressent généralement à deux types de ressources : le *temps* et l'*équipement*. Le temps est le temps passé par un attaquant pour réaliser une attaque, sans compter le temps d'étude. Les équipements comprennent des ordinateurs, des appareils électroniques, des outils matériels et du logiciel. Pour les objectifs de cette discussion,

- *en quelques minutes* signifie qu'une attaque peut réussir en moins de dix minutes ; *en quelques jours* signifie qu'une attaque peut réussir en moins d'un mois, et *en quelques mois* signifie qu'une attaque réussie nécessite au moins un mois.

- *Sans équipement* signifie qu'aucun équipement spécial n'est nécessaire pour effectuer une attaque ; *un équipement disponible* est un équipement disponible dans l'environnement d'exploitation de la cible d'évaluation, ou qui fait partie de la cible d'évaluation, ou qui est dans le commerce ; *un équipement spécial* est un équipement spécifique pour perpétrer une attaque.

c) Les *opportunités* recouvrent des facteurs qui peuvent généralement être considérés comme hors du contrôle de l'attaquant, tels que le cas où l'assistance d'une autre personne est nécessaire (collusion), la possibilité d'un concours de circonstances particulier (chance), et la possibilité et les conséquences de la capture d'un attaquant (détection). Ces facteurs sont difficiles à coter en règle générale. Le cas de collusion est traité ici, mais d'autres facteurs peuvent devoir être considérés. Les formes suivantes de *collusion* sont considérées : *seul* si aucune collusion n'est nécessaire ; *avec un utilisateur* si la collusion entre un attaquant et un utilisateur ordinaire de la cible d'évaluation est nécessaire pour que l'attaque réussisse ; et *avec un administrateur* si la collusion avec un utilisateur de confiance de la cible d'évaluation est nécessaire. Cette définition de la collusion suppose que l'attaquant n'est pas un utilisateur autorisé de la cible d'évaluation.

6.C.31 Les facteurs exposés ci-dessus ne sont pas supposés être définitifs ni complets ; ils sont seulement fournis à titre indicatif. Une fois que les facteurs ont été évalués pour un mécanisme particulier, les règles suivantes peuvent être utilisées pour calculer la résistance du mécanisme :

a) si le mécanisme peut être mis en échec par un profane en quelques minutes et sans équipement, alors, il n'atteint pas la cotation *élémentaire* ;

b) si le mécanisme ne peut être mis en échec que par un expert qui utilise un équipement spécifique, y consacrant des mois et avec la collusion d'un administrateur, alors le mécanisme atteint la cotation *élevée* ;

c) si le mécanisme ne peut être mis en échec qu'avec la collusion d'un utilisateur, le mécanisme atteint au moins la cotation *moyenne* ;

d) si le mécanisme ne peut être mis en échec qu'avec la collusion d'un administrateur, le mécanisme atteint au moins la cotation *élevée*;

e) si une attaque réussie nécessite des mois, le mécanisme atteint au moins la cotation *moyenne* ;

f) si une attaque réussie nécessite un expert, des mois d'effort et un équipement spécifique, alors le mécanisme est coté *élevée*, qu'une collusion soit nécessaire ou non ;

g) si une attaque réussie nécessite des jours d'effort, alors le mécanisme doit être au moins coté *élémentaire* ;

h) si une attaque réussie peut être réalisée en quelques minutes par toute personne autre qu'un profane, alors le mécanisme est coté *élémentaire* ;

i) si une attaque réussie nécessite un expert utilisant pendant des jours un équipement disponible, alors le mécanisme est coté *moyen*.

6.C.32 Au lieu d'évaluer ces prédicats, les évaluateurs peuvent utiliser les tables fournies en figures 6.C.5 et 6.C.6. Additionner les deux nombres trouvés en considérant le TEMPS et la COLLUSION en figure 6.C.5 et en considérant la COMPÉTENCE et l'EQUIPEMENT en figure 6.C.6 :

a) si le résultat est 1, alors la résistance n'est même pas *élémentaire* ;

b) si le résultat est supérieur à 1 mais inférieur ou égal à 12, alors la résistance est *élémentaire* ;

c) si le résultat est supérieur à 12 mais inférieur ou égal à 24, alors la résistance est *moyenne* ;

d) si le résultat est supérieur à 24, alors la résistance est *élevée*.

6.C.33 Les valeurs indiquées dans les figures 6.C.5 et 6.C.6 ne sont fournies que dans le but d'évaluer le prédicat. Elles n'ont aucune autre signification. Par exemple, un profane sans équipement disposant de quelques minutes et avec l'aide d'un utilisateur (valeur 13) n'est ni pire ni meilleur qu'un expert, seul, sans équipement, disposant de plusieurs mois/années (valeur 22) - les deux sont cotées *moyenne*.

Figure 6.C.5 Table temps/collusion

TEMPS	COLLUSION: seul	COLLUSION: avec un utilisateur	COLLUSION: avec un administrateur
minutes	0	12	24
jours	5	12	24
mois/années	16	16	24

Figure 6.C.6 Table compétence/équipement

COMPÉTENCE	ÉQUIPEMENT: sans équipement	ÉQUIPEMENT: utilisation d'un équipement disponible	ÉQUIPEMENT: utilisation d'un équipement spécial
profane	1	sans objet	sans objet
compétent	4	4	sans objet
expert	6	8	12

6.C.34 Ces tables ne devraient être utilisées qu'à titre de conseils puisqu'elles peuvent ne pas être applicables à tous les mécanismes et environnements d'exploitation. Ces tables ne doivent pas être utilisées pour coter des mécanismes cryptographiques (voir ITSEC paragraphe 3.23).

Annexe 6.D Analyse d'impact pour une réévaluation

Introduction

6.D.1 Il est illusoire de penser qu'une cible d'évaluation, son environnement opérationnel ou son environnement de développement ne seront pas amenés à changer. Il est beaucoup plus probable que l'enchainement des traitements liés au cadre de la sécurité des TI soit itératif et sans fin comme indiqué en partie 1 de l'ITSEM, figure 1.1.1.

6.D.2 Le résultat d'une évaluation s'applique uniquement à une révision ou version donnée d'un système ou d'un produit TI. Pour cette raison, tout changement de la cible d'évaluation ou des fournitures associées pourrait rendre nécessaire une réévaluation. Une évaluation complète à chaque changement n'est pas nécessaire et il est possible de bénéficier des résultats des évaluations précédentes. Comme l'impact d'un changement ne concerne pas toujours la sécurité, un processus, appelé analyse d'impact, est demandé pour indiquer les conséquences d'un changement dans les domaines précédemment cités, c'est-à-dire pour indiquer si ce changement impose une réévaluation.

6.D.3 Cette annexe offre des conseils élémentaires pour les commanditaires, les développeurs et les responsables de l'homologation de systèmes en décrivant le processus d'analyse d'impact qui aborde les sujets suivants :

a) comment établir la nécessité d'une réévaluation ;

b) comment identifier les parties de la cible d'évaluation qui sont touchées ;

c) quelles tâches de l'évaluation doivent être reprises.

6.D.4 La partie 3 de l'ITSEM (décrivant *la philosophie, les concepts et les principes*) et la partie 4 de l'ITSEM (décrivant *le processus d'évaluation*) constituent les bases de l'évaluation. Le chapitre 4.6 de la partie 4 qui traite de *la réutilisation* est en rapport direct avec cette annexe.

Analyse d'impact

Présentation générale

6.D.5 Le résultat d'une évaluation ne s'applique qu'à la révision et à la version d'une cible d'évaluation qui a été évaluée. Si une cible d'évaluation, son environnement opérationnel ou son environnement de développement sont changés par la suite, il est de la responsabilité du commanditaire de déterminer le type du changement et les conséquences induites pour le certificat/rapport de certification.

6.D.6 Selon le type de changement apporté, il peut être nécessaire que le commanditaire/ développeur en avertisse l'organisme de certification. Si une réévaluation est exigée, le commanditaire/développeur devra délivrer les fournitures pertinentes à un CESTI.

6.D.7 La règle principale de ce processus est que toutes les décisions devront être prises en fonction du niveau d'évaluation qui a été attribué à la cible d'évaluation. Comme le niveau d'évaluation attribué est une mesure de la confiance qui peut être accordée à une cible d'évaluation dans l'atteinte de ses objectifs de sécurité, il est nécessaire que tout changement soit examiné scrupuleusement avec le même degré de rigueur que pendant l'évaluation initiale. Dans le cas contraire, le niveau de confiance ne peut plus être maintenu.

6.D.8 Les changements apportés à l'environnement de développement ou à la plate-forme matérielle sont traitées de façon spécifique. Au cours du déroulement de l'évaluation, seront identifiés les outils qui touchent à la sécurité, comme par exemple le compilateur utilisé pour générer le code objet.

6.D.9 Comme les outils de développement utilisés ainsi que leur influence sur la confiance accordée à la cible d'évaluation sont très divers, aucun schéma universel relatif à leur traitement ne peut être développé. En conséquence, les changements de l'environnement de développement ou de la plate-forme matérielle doivent être traités au cas par cas. Il est du ressort de l'évaluation de déterminer les outils qui touchent à la sécurité en fonction du niveau d'évaluation de la cible. Si nécessaire, ils peuvent être enregistrés au chapitre 7 du RTE en même temps que d'autres informations utiles pour l'analyse d'impact.

Informations requises

6.D.10 Le processus d'analyse d'impact nécessite des informations qui concerne les composants de la cible d'évaluation et son environnement de développement. Si un commanditaire croit qu'une réévaluation est probablement nécessaire pour la cible d'évaluation, il devrait demander au CESTI d'enregistrer ces informations au chapitre 7 de l'ETR.

6.D.11 Une cible d'évaluation et son environnement de développement sont constitués d'un ensemble de composants coopérants, chacun d'eux ayant une des propriétés suivantes. Les types de composant sont définis ci-dessous (se référer à la partie 3 de l'ITSEM) :

a) SE : dédié à la sécurité (*Security Enforcing*) ;

b) SR : touchant à la sécurité (*Security Relevant*) ;

c) SI : ne touchant pas à la sécurité (*Security Irrelevant*).

6.D.12 Les exemples suivants s'appliquent uniquement aux exigences de confidentialité. Le composant d'un système d'exploitation qui assure l'identification et l'authentification réalise une fonction qui est dédiée à la sécurité et est par conséquent de type SE. L'ordonnanceur d'un système d'exploitation est un logiciel qui est touchant à la sécurité et est par conséquent de type SR. Le système de gestion mémoire ainsi que les données avec lesquelles il opère s'appuyant sur des microprogrammes et du matériel est touchant à la sécurité et est par conséquent de type SR. L'unité de calcul central (CPU) d'une machine, au travers d'une combinaison de logiciels et de microprogrammes est touchant à la sécurité et est par conséquent de type SR. Des programmes utilisateurs sans droit particulier sont de type SI.

Le processus

6.D.13 Le concept de processus d'analyse d'impact est présenté en figure 6.D.1. Il consiste en deux étapes, la première détermine le type de changement et la seconde permet de décider si une réévaluation est nécessaire et quelles sont les actions requises selon le type de ce changement.

Étape 1 (déterminer le type de changement)

6.D.14 Le type de changement apporté à la cible d'évaluation doit-être déterminé au moyen de la figure 6.D.2. Une description détaillée du processus ainsi que sa justification suivent.

6.D.15 Un changement peut être lié à la cible de sécurité, aux critères d'efficacité ou aux critères de conformité. Ce changement peut avoir des conséquences sur la confiance que l'on peut avoir dans une cible d'évaluation.

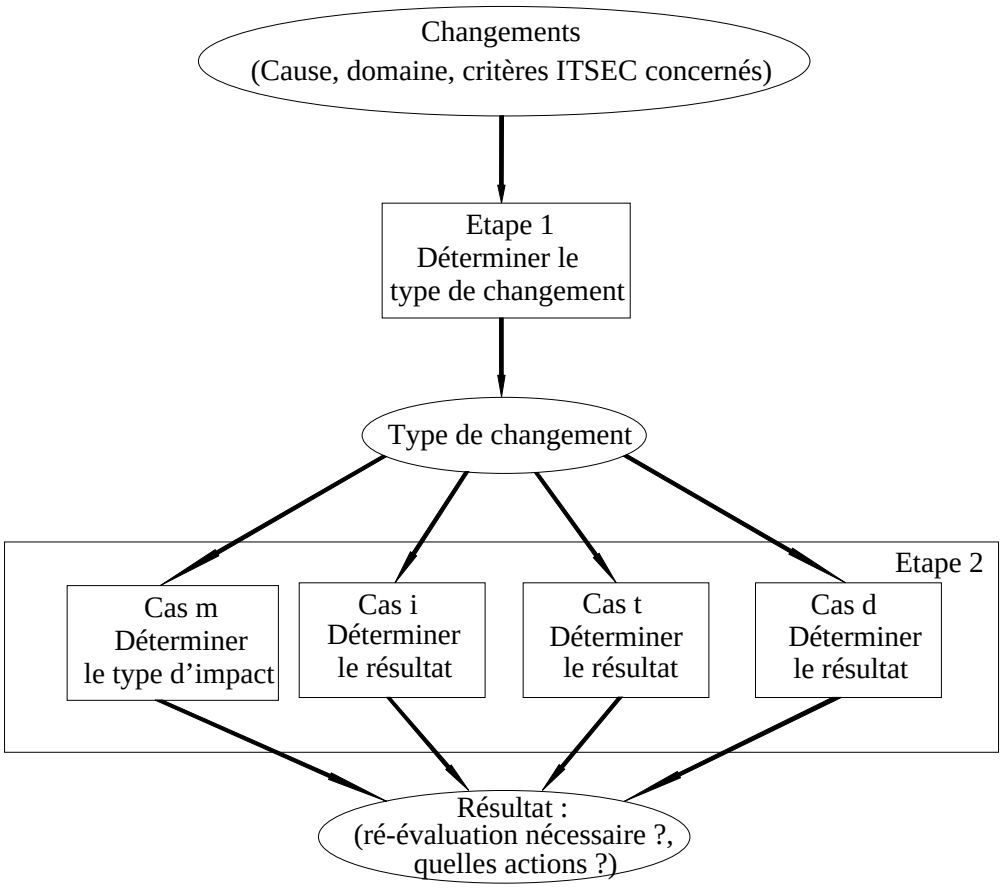


Figure 6.D.1 Vue générale du processus d'analyse d'impact

6.D.16 La figure suivante montre les causes possibles des changements apportés à une cible d'évaluation ainsi que leurs impacts. La figure comprend quatre colonnes : la cause du changement, le domaine auquel le changement se rapporte, les critères ITSEC concernés par le changement et le type de changement résultant.

6.D.17 Le type de changement peut prendre quatre valeurs :

m : pour un changement qui conduit finalement à une *modification* de la cible d'évaluation ;

i : pour un changement qui a seulement des effets *indirects* sur la cible d'évaluation ;

d : pour un changement de la *documentation* qui pourrait avoir des conséquences sur l'exploitation de la cible d'évaluation ;

t : pour un changement apportée à un *outil* (*tool*) utilisé au cours du développement.

Cause	Domaine	Critères ITSEC concernés	Type de modifi-cation
Ajout de nouvelles menaces Ajout de nouvelles fonctions dédiées à la sécurité Changement de la RdM	Cible de sécurité	Phase 1 - Spécification des besoins et/ou Phase 2 - Conception générale et/ou Phase 3 - Conception détaillée et/ou Phase 4 - Réalisation	m m m m
Découverte d'une vulnérabilité exploitable	Efficacité	Phase 1 - Spécification des besoins et/ou Phase 2 - Conception générale et/ou Phase 3 - Conception détaillée et/ou Phase 4 - Réalisation	m m m m
Changements du processus de développement	Conformité	Phase 1 - Spécification des besoins et/ou Phase 2 - Conception générale et/ou Phase 3 - Conception détaillée et/ou Phase 4 - Réalisation	m m m m
Changement de l'environnement de développement		Aspect 1 - Gestion de configuration Aspect 2 - Langages de prog. et compilateurs Aspect 3 - Sécurité des développeurs	i t i
Changement de la documentation d'exploitation		Aspect 1 - Documentation utilisateur Aspect 2 - Documentation d'administration	d d
Changement de l'environnement d'exploitation		Aspect 1 - Livraison et configuration Aspect 2 - Démarrage et exploitation	d d

Figure 6.D.2 Types de changement d'une cible d'évaluation

Étape 2 (déterminer le résultat)

6.D.18 Cette étape permet de déterminer le résultat, i.e. de déterminer si une réévaluation est nécessaire et quelles sont les actions nécessaires. Elle est divisée en quatre cas différents à exécuter en fonction du type de changement.

6.D.19 Dans cette section nous supposerons que le type des composants n'est pas changé. Ceci n'est pas toujours vrai. Par exemple, lors d'une réévaluation, des composants initialement considérés comme *touchants à la sécurité* peuvent devenir *dédiés à la sécurité* et vice versa. De plus, s'il y a un changement dans l'architecture, la séparation entre les composants dédiés à la sécurité, touchant à la sécurité et ne touchant pas à la sécurité peut être changée.

Cas m (déterminer le résultat pour un changement de type 'm')

6.D.20 Le changement de type m est divisée en quatre *sous-types de changement* définis ci-après :

m0 : un changement dans la cible de sécurité survient.

m1 : un changement au niveau de la conception générale survient sans que cela n'affecte la cible de sécurité.

m2 : un changement isolé survient au niveau de la conception détaillée. Ce changement n'a pas d'impact sur la conception générale et en conséquence une mise à jour des documents de conception générale n'est pas nécessaire.

m3 : un changement isolé survient au niveau de la réalisation. Ce changement n'a pas d'impact sur la conception détaillée et en conséquence une mise à jour des documents de conception détaillée n'est pas nécessaire.

6.D.21 Les contraintes additionnelles suivantes ont un impact sur le sous-type de changement. Si pour m2 ou pour m3, un changement ne peut pas être qualifié d'"isolé", c'est-à-dire s'il a un impact sur un certain nombre de composants de base, il faut appliquer le type de niveau le plus élevé le plus proche. Ainsi, un changement au niveau de la réalisation (m3) qui ne peut être qualifié d'"isolé" est équivalent à un changement de type m2. La même règle s'applique aux changements de type m2 qui deviennent de type m1. Les éléments de preuve qu'un changement est de type m0, m1, m2 ou m3 doivent être fournis par le commanditaire/développeur.

6.D.22 L'impact du type de changement est déterminé en utilisant la table appropriée selon le niveau d'évaluation de la cible comme indiqué en figure 6.D.3. Chacun des cinq types d'impact conduit à un résultat différent.

6.D.23 Il est nécessaire de disposer préalablement des éléments suivants comme donnée pour ce traitement :

a) le niveau d'évaluation atteint par la cible d'évaluation ;

b) le sous-type de modification (de m0 à m3) ;

c) le type (SE, SR, SI) du(des) composant(s) changé(s).

6.D.24 Le résultat de la table est le type d'impact associé à ce changement spécifique. Le type d'impact donne des indications sur les actions qui doivent être effectuées par le commanditaire/développeur et le CESTI.

Types d'impact

6.D.25 Le contenu des tables de la figure 6.D.3 distingue cinq valeurs possibles (types d'impact I1 à I5) qui montrent les conséquences d'un changement sur la cible d'évaluation évaluée. Il faut noter que le type d'impact peut changer après une analyse plus approfondie. Un récapitulatif des types d'impact est fourni en figure 6.D.4.

Niveau d'évaluation	Sous-type de changement
Type de composant	Type d'impact

E1	m0	m1	m2	m3
SE	I5	I4	I2	I2
SR	I5	I3	I2	I2
SI	X	I1	I1	I1

E2	m0	m1	m2	m3
SE	I5	I4	I3	I2
SR	I5	I3	I3	I2
SI	X	I1	I1	I1

E3	m0	m1	m2	m3
SE	I5	I4	I4	I3
SR	I5	I4	I3	I3
SI	X	I1	I1	I1

E4	m0	m1	m2	m3
SE	I5	I5	I5	I4
SR	I5	I4	I3	I3
SI	X	I1	I1	I1

E5	m0	m1	m2	m3
SE	I5	I5	I5	I4
SR	I5	I5	I4	I3
SI	X	I1	I1	I1

E6	m0	m1	m2	m3
SE	I5	I5	I5	I5
SR	I5	I5	I5	I4
SI	X	I1	I1	I1

'X' représente une combinaison impossible

Figure 6.D.3 Type d'impact pour E1 à E6

Figure 6.D.4 Récapitulatif des types d'impact	
Type d'impact	Actions nécessaires
I1	Informer l'organisme de certification
I2	I1 + fournir la documentation de test à l'organisme de certification
I3	délivrer les fournitures au CESTI Le CESTI vérifie le contenu, la présentation et les éléments de preuve
I4	I3 + le CESTI effectue toutes les tâches de l'évaluateur selon les critères ITSEC
I5	Réévaluation complète

Type d'impact I1

6.D.26 Les changements qui conduisent à un impact de type I1 ne sont pas touchant à la sécurité et aucune action n'est nécessaire sauf quand le changement a des conséquences sur le résultat de l'évaluation et du certificat/rapport de certification. Cependant le commanditaire/développeur doit informer l'organisme de certification en cas de doute.

Type d'impact I2

6.D.27 L'organisme de certification est informé du changement car il pourrait avoir un impact sur la mise en application de la politique de sécurité. Les documents de tests ainsi qu'une notification appropriée du changement au niveau d'évaluation, sont envoyés à l'organisme de certification.

Type d'impact I3

6.D.28 L'organisme de certification est informé du changement qui peut, lui aussi, avoir un impact sur la mise en application de la politique de sécurité. Les informations qui accompagnent la notification de changement doivent respecter les exigences concernant le contenu, la présentation et les éléments de preuve conformément au niveau d'évaluation, aux phases et aux aspects associés. Un CESTI vérifie que les informations fournies satisfont à toutes les exigences concernant le contenu, la présentation et les éléments de preuve relatives à la conformité et à l'efficacité. Les éléments de preuve qui concernent l'efficacité ne sont pas exigés pour les changements de type m2 dans la table associée à E2 et de type m3 dans la table associée à E3 (puisqu'ils ne sont pas exigibles lors de l'évaluation initiale).

Type d'impact I4

6.D.29 Les changements qui conduisent à un impact de type I4 affectent très probablement l'application de la politique de sécurité. Les mêmes règles que pour I3 s'appliquent mais les informations fournies dans le cadre I3 ne suffisent pas pour démontrer qu'après vérification le niveau d'évaluation reste toujours valide. Un CESTI doit réaliser les activités prévues par les tâches de l'évaluateur consignées dans les critères ITSEC, tant pour la conformité que pour l'efficacité, en fonction du niveau d'évaluation et de la phase. Si une erreur de conformité ou une vulnérabilité exploitable sont découvertes pendant le déroulement de cette activité, le type d'impact devient I5.

Type d'impact I5

6.D.30 Les changements qui conduisent à un impact de type I5 sont toujours touchant à la sécurité. L'organisme de certification est informé du changement. Les informations qui accompagnent la notification de changement doivent être suffisantes pour provoquer la tenue d'une réunion entre l'organisme de certification, le CESTI et le commanditaire. L'étendue de la réévaluation sera débattue pendant cette réunion. L'organisme de certification doit être averti de tout problème qui a donné lieu au changement proposé. Cette notification doit comprendre une liste des vulnérabilités mise à jour.

Notifications de changement

6.D.31 Les informations qui doivent être jointes à une notification de changement sont variables mais pour les impacts de I1 à I4 les informations suivantes sont nécessaires :

a) éléments de preuve que le changement est bien du type annoncé ;

b) éléments de preuve que le composant est bien du type annoncé ;

c) éléments de preuve appropriés pour le nouveau niveau d'évaluation de la cible.

6.D.32 Par exemple, les éléments de preuve pour le point c) comprennent les fournitures avec l'identification des changements, associées à une explication justifiant que les critères "isolé" et "sans impact au niveau de conception supérieur" sont satisfaits.

Cas i (déterminer le résultat pour un changement de type 'i')

6.D.33 Pour les changements de ce type, il faut vérifier si les exigences sont toujours valides en fonction du niveau d'évaluation de la cible.

Cas d (déterminer le résultat pour un changement de type 'd')

6.D.34 Il faut vérifier si le changement de la documentation a un impact sur les critères de *conformité - exploitation*, de *facilité d'emploi* ou de *vulnérabilité en exploitation*. Si ces critères ne sont pas affectés aucune action complémentaire n'est nécessaire. Dans le cas contraire, ils doivent être appliqués de nouveau.

Cas t (déterminer le résultat pour un changement de type 't')

6.D.35 Pour un changement de ce type, le résultat de l'évaluation reste valide si le niveau d'évaluation de la cible est inférieur ou égal à E2. Si il est supérieur ou égal à E3, il doit être vérifié pour le critère *langages de programmation et compilateurs* si le changement concret peut remettre en cause le niveau de confiance accordé à la cible d'évaluation.

Le processus de réévaluation

6.D.36 La réévaluation est réalisée après que l'opportunité en ait été jugée nécessaire et que les actions associées aient été décidées.

6.D.37 Comme le niveau d'évaluation est une mesure de la confiance que l'on peut avoir qu'une cible d'évaluation satisfasse ses objectifs de sécurité, il est indispensable que la réévaluation soit conduite avec le même degré de rigueur que l'évaluation initiale, voire même un degré de rigueur plus élevé si le niveau d'évaluation visé est plus élevé. Dans le cas contraire, le niveau de confiance ne peut pas être maintenu.

6.D.38 Il faut noter qu'il peut y avoir eu des améliorations apportées aux procédures de développement depuis l'évaluation initiale (par exemple, suite à des rapports d'anomalie). Ces changements peuvent affecter le niveau de travail que les évaluateurs peuvent considérer comme nécessaire pour cette réévaluation ou les futures réévaluations.

Annexe 6.E Conseils pour les distributeurs d'outils : construction d'un atelier d'évaluation

Introduction

6.E.1 Cette annexe décrit diverses idées pour la spécification et la construction d'un atelier d'évaluation. Les distributeurs ou les fournisseurs d'outils devraient prendre en compte ces concepts au cours de leur construction d'outils d'évaluation.

6.E.2 Les idées de base proviennent du monde de l'ingénierie du développement de logiciels. Le génie logiciel (GL) procure aux développeurs un ensemble d'outils qui mettent en oeuvre des méthodes destinées à la spécification, la conception, la programmation, au test et à la validation des logiciels. Un environnement intégré de soutien de projet (IPSE) est une plate-forme logicielle dans laquelle un développeur peut intégrer tous les outils dont il a besoin pour couvrir le cycle de développement dans son ensemble. L'intégration d'outils dans un IPSE en fait un atelier de génie logiciel (AGL ou PIPSE). Un atelier conçu sur un AGL permet d'offrir une méthodologie de développement (par exemple, une organisation) et un éventail d'outils de gestion destinés à produire du logiciel de qualité.

6.E.3 Le concept développé dans cette annexe est d'adapter ces principes pour la réalisation d'un atelier d'évaluation destiné aux évaluateurs avec des outils leur permettant de travailler efficacement et d'assurer que les principes de l'évaluation décrits dans la partie 3 de l'ITSEM sont suivis. Le plus grand défi demeure la diversité des évaluations qui peuvent être conduites selon les critères ITSEC et la difficulté à trouver des solutions communes qui couvrent tout le champ des TI. Cela pourrait être résolu par la tendance toujours plus grande à la normalisation et l'ouverture des systèmes dans ce domaine.

6.E.4 Le but de cette annexe est donc :

a) de présenter les concepts de base pour la réalisation d'AGL d'évaluation afin de montrer qu'il est possible de tirer des bénéfices d'un rapprochement étroit entre les techniques et les outils (décrits au chapitre 4.5, partie 4) pour la conduite d'une évaluation.

b) De donner les caractéristiques typiques attendues pour les outils destinés à peupler l'atelier de l'évaluateur. Aucune tentative n'est faite ici pour aborder les outils et les techniques spécifiques utilisées dans le développement de systèmes. Évidemment, l'atelier d'évaluation sera d'autant moins coûteux qu'il existera de nombreux points communs entre les outils de développement et les outils d'évaluation.

c) De fournir des informations complémentaires sur les catégories d'outils pour lesquelles le choix d'outils par les évaluateurs est difficile ; le contenu de cette section est susceptible d'évoluer du fait de l'évolution des TI.

Un AGL pour l'atelier d'évaluation

Concept

6.E.5 Il est bénéfique que les techniques et outils décrits dans le chapitre 4.5 de la partie 4 coopèrent afin de soutenir l'intégralité du processus d'évaluation. Pour y parvenir, ils peuvent être organisés à l'intérieur d'un IPSE. L'IPSE fournit une structure d'accueil (des formats définis pour l'échange de données, une base de données d'évaluation partagée, des services communs de traitement de textes, la manipulation et l'affichage de résultats, etc.) dans laquelle chaque outil pris individuellement peut être intégré.

6.E.6 Un AGL aborde les principaux problèmes posés par la productivité, la durée et la qualité des évaluations.

6.E.7 En accord avec les approches et les normes internationales et Européennes ([ECMA], par exemple), il est également important de viser une approche de système ouvert et de parler d'IPSE ou d'AGL d'évaluation ouverts. Finalement, il est utile d'inclure les outils de CAO pour le matériel ou d'autres outils spécifiques à une cible d'évaluation.

Avantages

6.E.8 Les avantages d'un AGL sont de faciliter :

a) la gestion du projet d'évaluation : estimation de délai et de coût, planification du projet d'évaluation, l'ordonnancement des activités d'évaluation, etc. ;

b) la gestion de configuration de l'évaluation : les tâches d'évaluation devraient être conduites à l'aide d'une gestion de configuration (aspect particulièrement important pour le traitement des corrections suites à des erreurs découvertes durant l'évaluation ainsi que dans le cas des réévaluations après modification de la cible d'évaluation) ;

c) la production et la gestion de la documentation de l'évaluation ;

d) les outils de communications entre AGL : il peut être utile de connecter entre-eux les évaluateurs qui ont à travailler sur la même cible d'évaluation voire, si les considérations de sécurité le permettent, deux CESTI ou plus ;

e) la création d'une base de données d'évaluation : des précautions doivent être prises lors de la collecte et du stockage d'informations dont les fournisseurs ont la propriété ;

f) d'autres services associés : par exemple, l'aide en ligne.

6.E.9 L'AGL pourra également bénéficier de l'intégration de nouveaux outils permettant l'automatisation du processus d'évaluation.

Architecture

6.E.10 La figure 6.E.1 propose une architecture générale en couche qui peut être utilisée pour développer un AGL d'évaluation. Cette architecture intègre :

a) un système d'exploitation qui fournit quelques mécanismes de sécurité de base destinés à protéger les informations propriétaires évaluées (par exemple, le code source) et les informations produites au cours du processus d'évaluation ;

b) une couche de services communs en support d'un environnement intégré de développement de logiciel (éventuellement commun à l'environnement de développement de la cible d'évaluation) fournissant la base pour intégrer des outils, par exemple [PCTE] ;

c) un fond de panier logiciel qui imposent l'homogénéité des méthodes et des outils et si nécessaire, des règles d'évaluations ;

d) un environnement horizontal fournissant les services de gestion élémentaires tels que des fonctions d'édition et de gestion de documentation, un outil de gestion de configuration, une gestion de projet, une messagerie ; cet environnement horizontal peut également recevoir les outils des développeurs nécessaires à l'évaluation (compilateurs, bibliothèques) ;

e) un environnement vertical dans lequel s'inscriront les différents outils d'évaluation (comme décrit dans le chapitre 4.5, partie 4) ;

f) une interface homme-machine conviviale.

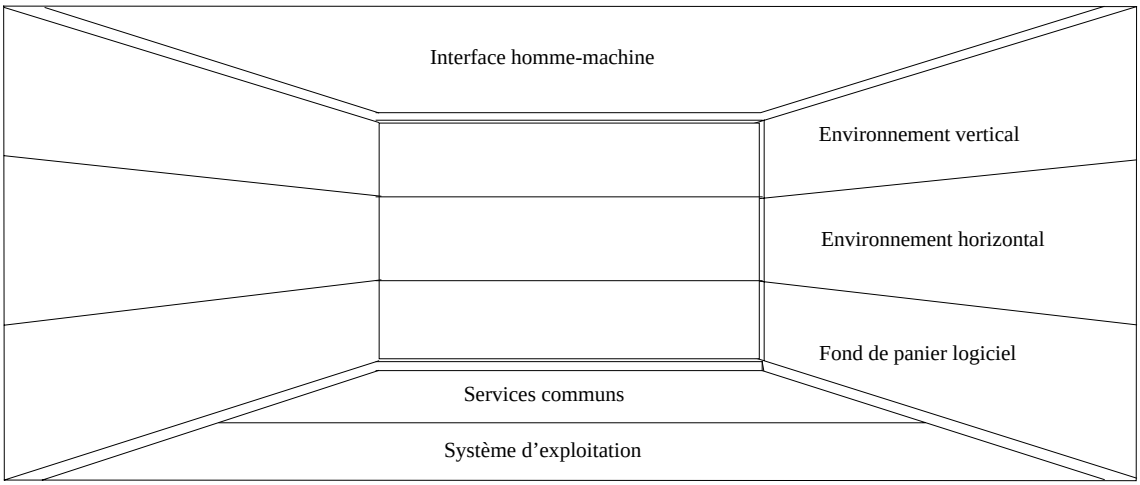


Figure 6.E.1 Architecture possible d'un AGL

Listes de contrôle

6.E.11 Il est nécessaire de s'assurer que les CESTI prennent en compte tous les éléments pertinents lors de l'application de chaque critère ITSEC. Les ITSEC ne fournissent pas de liste de contrôle générale parce que les tâches de l'évaluateur spécifiques seront régies par la nature de la cible d'évaluation et ses exigences de sécurité telles que définies dans sa cible de sécurité.

6.E.12 L'atelier peut aider à la génération et à la validation de listes de contrôles cohérentes entre différentes évaluations en sorte que si deux CESTI avaient à évaluer la même cible d'évaluation par rapport à la même cible de sécurité, ils généreraient les mêmes listes de contrôle.

Peuplement d'un atelier d'évaluation

Généralités

6.E.13 Cette section décrit les caractéristiques souhaitables des outils d'évaluation. Elle traite essentiellement des caractéristiques aidant au respect des principes de ***répétabilité***, ***reproductibilité*** et ***objectivité***.

Pertinence technique des outils

6.E.14 La pertinence technique d'un outil peut être caractérisée par son champ d'application et le degré de précision obtenu.

6.E.15 *Champ d'application* : la génération d'outils destinés aux activités d'évaluation peut suivre deux approches : la première tente de créer des outils qui sont aussi universels que possible ; la seconde tente de créer un ensemble d'outils spécialisés.

6.E.16 Les outils spécialisés ont l'inconvénient d'être d'application limitée et de manquer de souplesse. Ainsi, il peut être difficile d'utiliser effectivement des outils spécialisés. Avec le progrès de la normalisation dans le domaine des TI et une meilleure définition des tâches de l'évaluateur, le domaine des outils spécialisés prendra de l'importance.

6.E.17 La possibilité de combiner l'utilisation de plusieurs outils est particulièrement importante pour l'évaluation dans des domaines où l'outil pertinent unique n'existe pas. La structure d'un AGL permet des combinaisons souples et efficaces.

6.E.18 *Degré de formalisation* : pour des niveaux d'évaluation élevés, les outils doivent pouvoir prendre en compte des méthodes semi-formelles ou formelles que les critères ITSEC exigent. Les propriétés de ces outils peuvent être caractérisées comme suit :

a) leurs langages de données ont une syntaxe et une sémantique parfaitement définies ;

b) la validité des résultats qu'ils produisent repose sur une théorie mathématique ou un modèle formel.

Facilité d'apprentissage et d'utilisation des outils

6.E.19 La technique sous-jacente sur laquelle se base l'outil doit être facile à apprendre et facile à utiliser afin d'éviter les malentendus et les erreurs de raisonnements. Cela n'implique pas que la technique elle-même soit simple. Même lorsque les techniques sont complexes où reposent sur une théorie complexe, les évaluateurs doivent être capables d'utiliser l'outil effectivement. La formation est un élément clef pour y parvenir.

6.E.20 *La facilité d'apprentissage* est une exigence de fond. Même si la tâche à automatiser est complexe un outil devrait permettre d'obtenir des résultats utiles. Les facteurs qui affectent la facilité d'apprentissage sont :

a) la qualité et la pertinence de la documentation (y compris les messages d'erreur et l'aide en ligne) ;

b) la qualité de la formation ;

c) la conception de l'interface homme-machine ;

d) le respect des normes.

6.E.21 La documentation devrait être complète, incluant un guide et des exemples d'utilisation en évaluation.

6.E.22 *La facilité dans la préparation des données* : il est souhaitable que l'outil soit aussi souple que possible en acceptant divers formats de données.

6.E.23 *La facilité d'interaction* améliore l'efficacité des évaluateurs. La prise en compte des aspects suivants facilite l'interaction, et par la même, améliore la pertinence de l'outil :

a) l'affichage ;

b) la structure des commandes (i.e. menus, invites) et comment les nommer au mieux.

Exigences sur les résultats des outils

6.E.24 *Pertinence des résultats* : l'à-propos et la clarté des résultats améliore la pertinence d'un outil. La facilité d'interprétation des résultats d'un outil est influencée par les mêmes facteurs que ceux qui influencent la facilité de la préparation des données et la facilité d'interaction. La clarté des résultats peut avoir un impact significatif sur l'utilité de l'outil.

6.E.25 Quels que soient les types de résultats, ils devraient être bien présentés. Les résultats d'ensemble devraient être délivrés simplement, en présentant des conclusions précises.

6.E.26 Les exigences des résultats sont abordées sous les rubriques suivantes : *enregistrement des activités de l'évaluateur, conclusions affirmatives* et *validité des résultats.*

6.E.27 *Enregistrement des activités de l'évaluateur* : les exigences pour l'enregistrement des activités de l'évaluateur sont particulièrement importantes en cas d'utilisation d'outils interactifs. Un moyen de répéter l'application de l'outil est exigé en sorte qu'un résultat puisse être démontré aux autres évaluateurs ou aux autres parties. Pour y parvenir, l'outil pourrait enregistrer chaque séquence de commandes entrée afin d'être en mesure de les rejouer manuellement ou, de préférence, automatiquement (il peut s'agir d'un mécanisme standard de l'atelier lui-même). Un enregistrement détaillé des activités de l'évaluateur est un des premiers avantage de l'automatisation du processus d'évaluation.

6.E.28 *Conclusions affirmatives* : si le résultat de l'outil est une déclaration qu'un résultat judicieux est maintenu, alors c'est un net avantage sur l'outil qui se contente de ne pas indiquer le contraire.

6.E.29 *Absence de conclusions négatives* : si un outil est conçu pour chercher certaines caractéristiques indésirables, il est important que l'absence de ces caractéristiques soit facile à observer. L'absence de conclusions négatives fournit des éléments de preuve pour le processus d'évaluation, mais ne suffit pas pour garantir l'absence de vulnérabilité. Ces deux cas peuvent être difficile à observer si le résultat n'est pas probant.

6.E.30 *Validité des résultats* : les résultats de l'outil doivent être dignes de confiance ; si les éléments de preuves sont fournis par un outil mettant en œuvre un système formel, cette confiance pourra être établie en terme de bien-fondé. C'est-à-dire que l'on aura davantage confiance en un outil qui n'est capable de démontrer que des résultats "vrais" qu'en un outil capable d'en démontrer aussi des "faux".

Viabilité commerciale des outils

6.E.31 Finalement, il est souhaitable de n'utiliser que les outils qui ont de bonnes caractéristiques commerciales ; ces caractéristiques comprennent la portabilité, la maintenance et l'évolutivité.

6.E.32 *Portabilité* : la portabilité d'un outil a trait à sa disponibilité sur différents systèmes d'exploitation et différents types de matériels. La portabilité est un avantage majeur pour l'évaluation étant donné la diversité des systèmes d'exploitation utilisés. Cependant la question "Un portage produit-il un outil identique ?" doit être abordée.

6.E.33 *Maintenabilité* : il est important que l'outil reste utilisable en cas de mise à niveau du système. Continuer à le maintenir est une réelle exigence vis-à-vis du fournisseur de l'outil.

6.E.34 *Évolutivité* : les outils évoluent avec les techniques qu'ils mettent en œuvre. Des fonctionnalités améliorées peuvent être ajoutées mais pour des raisons de répétabilité, les modifications dans un outil ne devraient pas modifier le caractère applicable des résultats précédemment produits avec cet outil.

Annexe 6.F Modèle de composition et exemple d'application

Objet

6.F.1 Cette annexe s'adresse aux commanditaires, aux intégrateurs et aux responsables de l'homologation de systèmes qui sont concernés par la composition de cibles d'évaluation déjà évaluées.

6.F.2 L'objectif de cette annexe est de :

a) décrire un modèle de composition de cibles d'évaluation déjà évaluées ;

b) décrire à l'aide d'exemples comment utiliser ce modèle.

6.F.3 Étant donné la complexité du cas général, seul un modèle simplifié peut être décrit. Des conseils supplémentaires à ce sujet devraient être obtenus auprès des organismes de certification.

Sommaire

6.F.4 Cette annexe débute par la description d'un modèle simple de composant et montre alors comment le modèle peut être utilisé pour décrire la composition de deux composants déjà évalués.

6.F.5 Comme les possibilités de composition sont nombreuses, deux cas de composition sont proposés pour montrer les propriétés pertinentes de la composition.

6.F.6 L'expérience pratique de la composition de produits évalués est limitée.

Le modèle de composition

6.F.7 Dans le contexte de la composition, le terme *composant* est utilisé dans cette annexe pour faire référence à un composant déjà évalué utilisé dans la construction de la cible d'évaluation. L'utilisation de ce terme est en accord avec la définition des critères ITSEC (i.e. un composant est une partie identifiable et autonome d'une cible d'évaluation) puisque le résultat de la composition est lui-même une cible d'évaluation.

6.F.8 Un composant est vu comme une "boîte blanche" (ce qui signifie que sa structure interne est connue jusqu'à un certain niveau de détail qui dépend du niveau de l'évaluation) par opposition à "boîte noire" pour laquelle la structure interne n'est pas connue.

6.F.9 Un composant dans le modèle est décrit par :

a) un ensemble de prédicats P qu'il satisfait ;

b) une interface qui fournit des services à l'environnement dans lequel le composant réside et une interface pour la fourniture de services au composant ;

c) des hypothèses sur l'environnement dans lequel réside le composant ;

d) des détails sur sa structure interne.

6.F.10 L'ensemble des prédicats P est directement lié à la fonctionnalité du composant. Cette fonctionnalité peut être soit dédiée à la sécurité (elle est liée à la cible de sécurité), soit touchant à la sécurité (par exemple, elle est le support d'une fonction dédiée à la sécurité). L'ensemble des prédicats peut couvrir un domaine allant de la description d'une politique de sécurité complète jusqu'à la description d'une propriété nécessaire d'un composant exprimée par un seul prédicat.

6.F.11 Les services fournis par l'interface sont soit utilisés par un autre composant, soit fournis à un utilisateur. Cette interface peut être appelée interface producteur. Le niveau de détail de la description de l'interface et de la description des services rendus dépend du niveau de l'évaluation.

6.F.12 Deux types d'hypothèses sur l'environnement sont possibles :

a) Un sous-ensemble peut décrire les services externes non TI nécessaires sur lesquels repose le fonctionnement sûr du composant (le fonctionnement sûr recouvre la conformité et l'efficacité dans les termes des critères ITSEC).

b) L'autre sous-ensemble peut décrire les services externes TI nécessaires sur lesquels repose le fonctionnement sûr du composant. Pour ces services TI, une description d'interface ainsi qu'une description des services attendus sont nécessaires. Cette interface peut être appelée interface consommateur du composant.

6.F.13 Toutes les combinaisons arbitraires d'hypothèses sont possibles. Par exemple, un système de gestion de base de données peut faire des hypothèses strictement TI concernant la fournitures de services par un système d'exploitation sous-jacent. Alors que le système d'exploitation sous-jacent peut faire des hypothèses non TI concernant la sécurité physique de l'environnement dans lequel il opère.

6.F.14 La structure interne est décrite avec une finesse qui dépend du niveau d'évaluation. La structure interne est une source de vulnérabilités.

6.F.15 La représentation schématique d'un composant est donnée en figure 6.F.1.

6.F.16 Une combinaison de composant peut être décrite en utilisant la définition du modèle de composant proposée précédemment. Pour simplifier la présentation qui suit, on pose que l'ensemble des hypothèses concernant les services non TI est vide.

Combinaison de composants - 1er cas

6.F.17 Le composant C1 utilise les services produits par le composant C2. Une interface visible extérieurement est fournie par le composant C1. C2 présente une interface producteur au composant C1 mais cette interface n'est pas visible par un utilisateur.

6.F.18 Exemple pour le 1er cas :

a) composant C1 - client ;

b) composant C2 - serveur.

6.F.19 Une représentation schématique du 1er cas se trouve en figure 6.F.2. La flèche entre les deux composants pointant sur le composant C2 doit être interprétée comme : C2 est utilisé par C1.

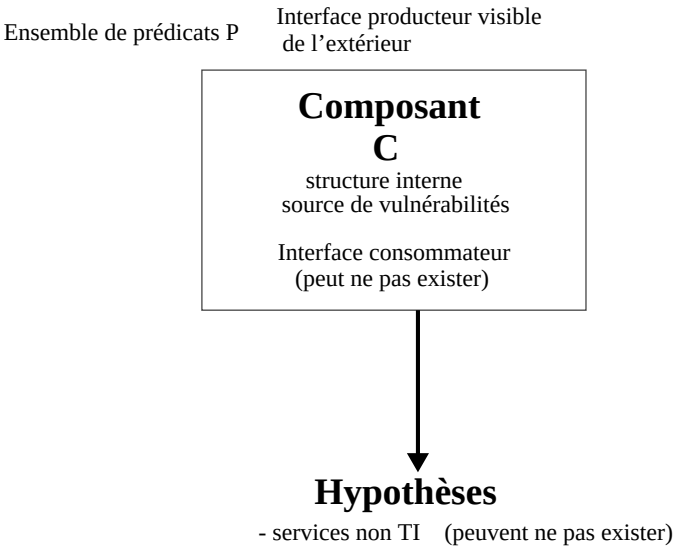


Figure 6.F.1 Un composant d'une cible d'évaluation

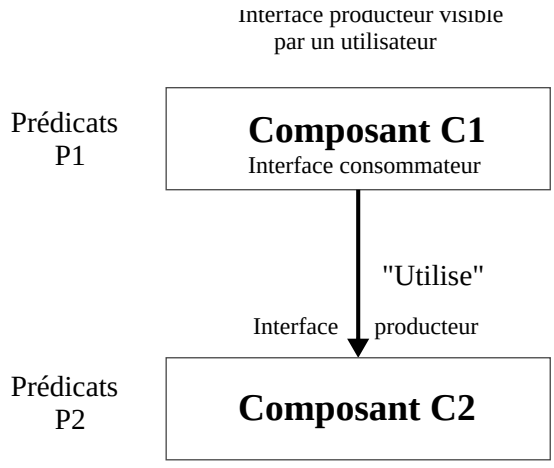


Figure 6.F.2 Combinaison de composants ; 1er cas

Combinaison de composants - 2ème cas

6.F.20 Le composant C1 utilise les services produits par le composant C2. Les interfaces visibles de l'extérieur sont présentées par les composants C1 et C2.

6.F.21 Exemple pour le 2e cas :

a) composant C1 - moniteur de machine virtuelle ;

b) composant C2 - plate-forme matérielle.

6.F.22 L'interface visible est fournie par les instructions machines de l'interface du moniteur de machine virtuelle et de la plate-forme matérielle.

6.F.23 Une représentation schématique du 2e cas se trouve en figure 6.F.3.

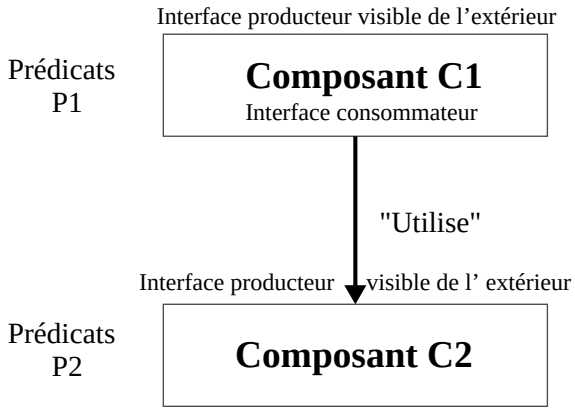


Figure 6.F.3 Combinaison de composants ; 2ème cas

Combinaison de composants - 3ème cas

6.F.24 Le composant C1 utilise les services produits par le composant C2 et le composant C2 utilise les services produits par C1. Les interfaces visibles de l'extérieur sont présentées par les composants C1 et C2.

6.F.25 Une représentation schématique du 3e cas se trouve en figure 6.F.4.

Compositions résultant de l'application du modèle

6.F.26 Dans toutes les combinations le composant résultant est appelé C3. Il a son propre ensemble de prédicats P3 et toutes les autres caractéristiques d'un composant telles que son interface producteur, sa structure interne, etc.

6.F.27 Par exemple, si la combinaison correspond au 1er cas, les conditions suivantes doivent être vérifiées pour que les prédicats P3 soient satisfaits par le composant C3 :

Condition 1 : C1 doit être correctement réalisé.

Condition 2 : C2 doit être correctement réalisé.

Condition 3 : L'interface consommateur de C1 doit correspondre exactement à l'interface producteur de C2.

Condition 4 : Les prédicats P3 sont le résultat de la combinaison des prédicats P1 et P2. Cela signifie que P3 est dérivé de P1 et P2.

Condition 5 : Les prédicats P2 doivent rester satisfaits en dépit de toute vulnérabilité de C2. Il faut donc montrer que les vulbérabilités de C2 ne sont pas exploitables vis-à-vis des prédicats P2.

Condition 6 : Les prédicats P1 doivent rester satisfaits en dépit de toute vulnérabilité de C1. Il faut donc montrer que les vulbérabilités de C1 ne sont pas exploitables vis-à-vis des prédicats P1.

Condition 7 : Il faut montrer que les vulnérabilités de C2 ne sont pas exploitables vis-à-vis des prédicats P1.

Condition 8 : La relation "utilise" est vraiment dirigée uniquement du composant C1 vers le composant C2 (elle est unidirectionnelle).

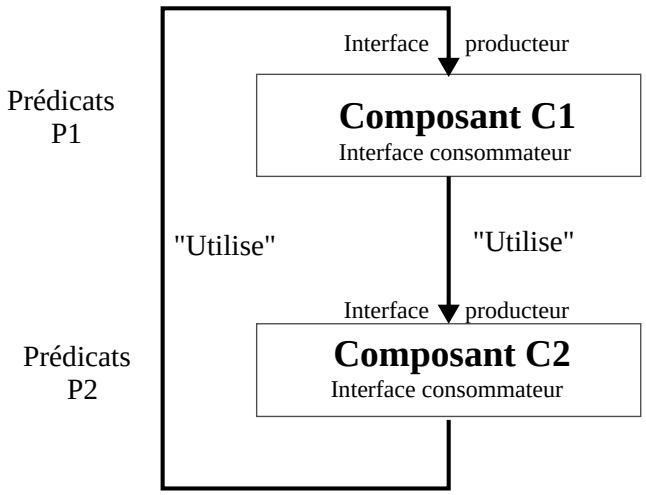


Figure 6.F.4 Combinaison de composants ; 3ème cas

6.F.28 Ce qui suit est une liste des problèmes possibles dans ce cas de figure :

a) La confiance en la véracité de la condition 1 est différente de la confiance en la véracité de la condition 2. C'est la cas ou le composant C1 a été évalué à un niveau différent du composant C2.

b) La condition 3 n'est pas vraie. Les causes possibles sont :

- l'interface consommateur de C1 est un sous-ensemble de l'interface producteur de C2 ;

- l'interface consommateur de C1 est un sur-ensemble de l'interface producteur de C2 ;

- les interfaces consommateur (C1) et producteur (C2) sont décrites à des niveaux de détail différents.

c) Comment démontrer que les prédicats P1 et P2 constituent P3 quand P1 et P2 peuvent être n'importe quel ensemble de prédicats ?

d) La confiance en la véracité de la condition 5 est différente de la confiance en la véracité de la condition 6. C'est encore un cas où les composants C1 et C2 ont été évalués à des niveaux différents.

e) Il faut démontrer, au niveau d'évaluation spécifié, que la relation "utilise" est unidirectionnelle, comme prévu.

6.F.29 Si la finesse des représentations des entités est différente, ce qui est normalement le cas lorsqu'elles sont à différents niveaux d'abstraction, alors on peut trouver une transformation telle que les prédicats du composant C1 et du composant C2 référencent au moins les mêmes entités. Les prédicats P1' obtenus peuvent alors être étudiés pour vérifier s'ils constituent avec P2 les prédicats P3 de la combinaison. Il est essentiel d'identifier toutes les contradictions des deux ensembles de prédicats.

6.F.30 Étant donné la nature arbitraire des prédicats P1 et P2, aucune règle générale ne peut être donnée pour déterminer si les prédicats P1 et P2 constituent les prédicats P3 ni comment ils le constituent.

Index

Les termes provenant du glossaire de l'ITSEC sont précédés de : ❍

Page laissée blanche.