Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général
de la défense
et de la sécurité nationale

*Agence nationale de la sécurité
des systèmes d'information*

Paris, le 16 juillet 2010

N° 1897/ANSSI/SR

Référence : ANSSI-CC-NOTE/07.1

NOTE D'APPLICATION

INTERPRETATION DES CRITERES COMMUNS POUR LES EVALUATIONS DE SYSTEMES

Application : Dès son approbation.

Diffusion : Publique.

Le directeur général
de l'agence nationale de la sécurité
des systèmes d'information

Patrick PAILLOUX

[ORIGINAL SIGNE]

Suivi des modifications

Edition	Date	Modifications
1	16/07/10	Première édition officielle.

En application du décret n° 2002-535 du 18 avril 2002, la présente note a été soumise au comité directeur de la certification, qui a donné un avis favorable.

TABLE DES MATIERES

1. Objet de la note

L'objet de la présente note est de fournir une approche du concept d'évaluation "système" afin d'obtenir un certificat "Critères Communs" qui atteste l'atteinte d'un niveau EAL.

En effet, les Critères Communs, conçus pour réaliser l'évaluation de produits des technologies de l'information, ne font pas apparaître clairement, à la différence des ITSEC, ce qu'est un système et comment, en pratique, on peut l'évaluer.

Il est précisé que les évaluations de systèmes sont réalisées dans le même cadre procédural que les évaluations de produits (voir la procédure ANSSI-CC-CER/P/01, disponible sur www.ssi.gouv.fr).

2. Références

- [CC v3.1rx] :
  Les différentes révisions des CC v3.1, à savoir, à la date de publication de la présente note :
  - Critères Communs Parties 1-2-3 et CEM ; Version 3.1, Révision 1 ; juin 2006 ; Réf. : CCMB-2006-06-001 à 004
  - Critères Communs Parties 1-2-3 et CEM ; Version 3.1, Révision 2 ; juin 2006 et septembre 2007 ; Réf. : CCMB-2006-06-001 et CCMB-2007-09-002 à 004
  - Critères Communs Parties 1-2-3 et CEM ; Version 3.1, Révision 3 ; juillet 2009 ; Réf. : CCMB-2009-07-001 à 004
- [CC v2.x] :
  - Critères Communs Parties 1-2-3 et CEM ; Version 2.1 ; août 1999 ; Réf. : CCIMB-99-031, CCIMB-99-032, CCIMB-99-033 et CEM-99/045
  - Critères Communs Parties 1-2-3 et CEM ; Version 2.2 ; janvier 2004 (Révision 256) ; Réf. : CCIMB-2004-01-001 à 004
  - Critères Communs Parties 1-2-3 et CEM ; Version 2.3 ; août 2005 ; Réf. : CCMB-2005-08-001 à 004
- [ITSEC] : Critères d'Evaluation de la sécurité des technologies de l'information, version 1.2, juin 1991, office des publications officielles des communautés européennes.

3. Définition d'un système

Un système est une installation spécifique de produits des technologies de l'information (TI) dans un contexte d'exploitation connu.

Un système est construit à partir d'un certain nombre de composants matériels et logiciels (les produits TI). Certains composants sont réalisés spécialement, d'autres sont des produits standards. L'installation spécifique de ces produits TI correspond à leur configuration technique.

Le contexte d'exploitation correspond aux mesures de sécurité physiques, humaines et organisationnelles qui s'appliquent au système, comme par exemple :

- mesures de sécurité physiques : emploi de badgeuses, de barrières infrarouges, d'une surveillance vidéo, etc. ;
- mesures de sécurité humaines : formation des utilisateurs finaux du système, formation des administrateurs du système, etc. ;
- mesures de sécurité organisationnelles : attribution de droits d'accès au système, etc.

La notion de contexte d'exploitation correspond à celle d'environnement opérationnel qui est définie dans les [CC v3.1rx].

Dans le reste du document, on différencie la partie technique d'un système (i.e. partie TI) de sa partie non technique (i.e. le contexte d'exploitation).

4. Particularité de l'évaluation d'un système par rapport à une évaluation de produit

Du point de vue de la sécurité, la principale différence entre système et produit est que, dans le cas d'un système, le contexte d'exploitation, sur le périmètre identifié dans la cible de sécurité, est clairement défini et parfaitement maîtrisé, et qu'il est conçu pour satisfaire les besoins d'un groupe particulier d'utilisateurs finaux. Un produit, au contraire, considère toujours un environnement de déploiement supposé (environnement opérationnel qui sera décrit au chapitre "Restriction d'usage" du rapport de certification).

De plus, l'environnement d'exploitation d'un produit est entièrement sous la responsabilité de l'utilisateur final ,alors que dans le cas d'un système, le développeur[1] (en qualité de fournisseur du service) peut en être en partie responsable.

Il est donc supposé dans cette note que le client et le développeur se sont accordés en amont sur la cible de sécurité et sur le contexte d'exploitation, et que le développeur fournit les éléments de preuves appropriés au cours de l'évaluation (cf. § 6.1).

Du point de vue de l'évaluation, la principale différence réside dans l'évaluation de guides supplémentaires qui établissent les mesures de protection du contexte d'exploitation.

Par ailleurs, il est à noter que l'évaluation d'un système TI à haut niveau de confiance est une opération difficilement réalisable pour plusieurs raisons :

- en supposant que toute la documentation attendue soit disponible, il est humainement difficile d'appréhender l'intégralité du système TI du point de vue de la sécurité ;
- en général, la documentation attendue pour évaluer l'intégralité du système TI n'est pas disponible. Si le système TI est composé de produits TI non évalués ou dont la documentation de conception n'est pas disponible, on se trouve alors dans une impasse (à noter que le seul fait que les produits TI sont évalués ne suffit pas : il faudra s'assurer que les fonctions de sécurité du produit qui ont été évaluées correspondent à celles identifiées dans l'évaluation système, et que le produit est déployé conformément aux contraintes identifiées dans son rapport de certification).

C'est pourquoi, le plus souvent, l'évaluation système TI n'est envisagée qu'à des niveaux de confiance limités correspondant à ce qu'il est réaliste d'attendre en termes de fournitures.

5. Portée de la certification

La certification d'un système TI porte sur le système évalué et testé, considéré dans son environnement prévu d'utilisation.

Le système TI testé peut n'être qu'une représentation significative du système TI réel.

[1] Dans le reste de ce document on désigne par "développeur" le développeur du système, que celui-ci conçoive de nouveaux logiciels ou équipements, ou qu'il ne réalise que l'intégration de logiciels et équipements sur étagère.

On désigne par "client" l'ensemble des groupes d'utilisateurs finaux du système. Un système peut avoir plusieurs clients distincts.

Les évolutions du système peuvent être également certifiées, à la condition qu'elles soient réalisées conformément à des procédures évaluées (NB : l'ensemble des procédures évaluées sera identifié dans le rapport de certification du système).

Si des guides relatifs à l'évolution du dimensionnement du système ont été évalués, le rapport de certification précisera également les évolutions réalisées conformément à ces guides (la fiche de version restant toujours valide pour ces évolutions).

6. Tâches d'évaluation

Ce chapitre indique ce que le centre de certification attend au titre d'une évaluation système, tant du développeur que de l'évaluateur, en fonction des différentes familles d'assurance définies par les [CC v3.1rx] (la correspondance avec les [CC v2.x] des concepts présentés ici est fournie en Annexe A).

Ce paragraphe décrit tout d'abord les concepts particuliers mis en œuvre dans une évaluation système, puis les tâches à mener dans le cadre d'une évaluation système de bas niveau de confiance (niveau EAL1 et EAL2). Pour les évaluations de niveau plus élevé, il est nécessaire de contacter le centre de certification.

6.1. Eléments de preuve spécifiques à fournir dans le cadre d'une évaluation système

Comme mentionné plus haut, un système est défini comme une installation spécifique[2] de TI, et un contexte d'exploitation (non TI) particulier.

La figure suivante identifie synthétiquement les éléments spécifiques, par rapport à une évaluation produit, qui doivent être fournis dans le cadre d'une évaluation système. Ces éléments sont ceux présentés par les cases claires de la figure. Ils correspondent au contexte d'exploitation du système.

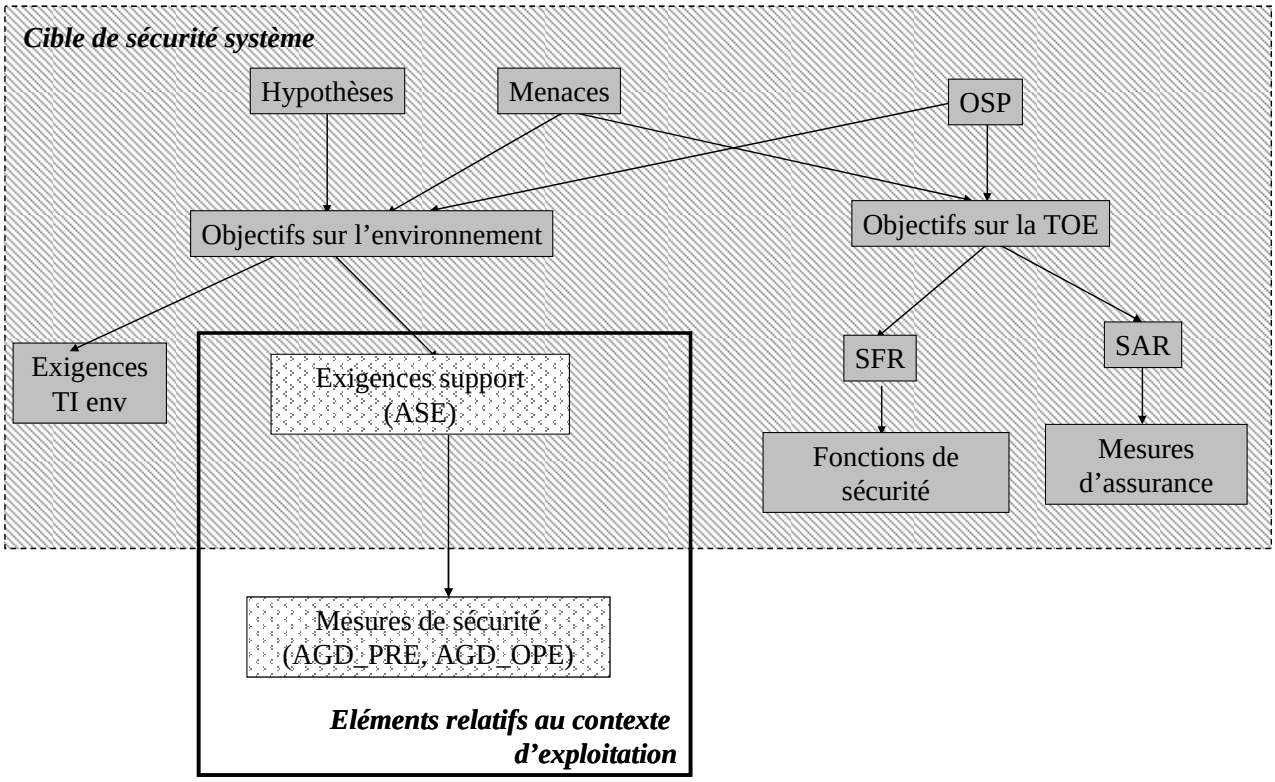

Figure 1 Spécificités des éléments de preuve d'une évaluation système

[2] Qui correspond à une configuration particulière (figée) des produits TI formant le système.

Au niveau de la cible de sécurité, le contexte d'exploitation est représenté par des « exigences support ». La déclinaison de ces exigences dans les guides du système est identifiée par des « mesures de sécurité sites ».

Le contexte d'exploitation est formalisé dans la cible de sécurité par des hypothèses et des politiques de sécurité organisationnelles (OSP), qui sont elles-mêmes raffinées en exigences support. (NB : Le terme « exigence » employé ici, ne désigne pas des exigences issues de la partie 2 des CC ; aucun formalisme spécifique n'est imposé ici pour exprimer ces exigences). Si les exigences support concernent des rôles ou phases spécifiques cela devra être présenté dans la cible de sécurité.

Le besoin de sécurité et sa couverture (éléments permettant de s'assurer que la problématique de sécurité est correctement couverte) doivent rester compréhensibles dans la cible de sécurité. La complexité de la cible de sécurité ne doit pas la rendre difficile à appréhender

On distingue les « exigences support développeur » des « exigences support clients ». Cette distinction permet d'établir la responsabilité de la mise en œuvre de ces mesures de sécurité. La répartition de ces responsabilités dépend du contrat qui est négocié entre ces deux parties.

Les exigences support sont ensuite déclinées en mesures de sécurité également sous la responsabilité de l'une des deux parties. Ces mesures de sécurité sont applicables aux sites où le système est déployé. Parmi ces sites, certains sont sous la responsabilité du développeur et d'autres sous la responsabilité du client. Le CESTI n'a pas à se préoccuper de cette répartition. Il devra juste s'assurer, au titre du composant AGD, que l'ensemble des mesures nécessaires à la protection du système a bien été défini.

6.2. Evaluation de bas niveau

Les paragraphes suivants identifient les spécificités de l'application des classes d'assurance CC dans le cadre d'une évaluation système de bas niveau.

Les tâches d'évaluation identifiées dans la CEM sont toutes appliquées. Cette note ne précise que les tâches d'évaluation supplémentaires.

a) Cible de sécurité (ASE)

La principale différence entre une cible de sécurité système et une cible plus traditionnelle est que ce document doit, dans le cas d'un système, décrire les caractéristiques du déploiement de ce système.

L'évaluateur doit vérifier que le contexte d'exploitation et les exigences de sécurité techniques couvrent le besoin de sécurité défini par les objectifs de sécurité de la cible de sécurité. Le rapport ASE doit identifier les objectifs de sécurité portant sur le système dans sa globalité. Pour faciliter le déroulement de l'évaluation, le rapport doit préciser comment la partie TI du système et son contexte d'exploitation contribuent à la couverture des objectifs. L'évaluateur devra également vérifier que toutes les hypothèses et OSP ne relevant pas de mesures TI sur l'environnement sont correctement déclinées en exigences support. En revanche, il n'est pas du ressort de l'évaluateur de se prononcer sur la répartition de ces exigences support entre le développeur et le client. L'évaluateur doit émettre un avis quant à la suffisance et la pertinence des exigences support pour couvrir les besoins de sécurité du contexte d'exploitation du système TI.

L'identification de la TOE est traitée au § 6.2.d, par ALC_CMC et ALC_CMS.

Bien que la description des exigences sur l'environnement ne soit plus requise par les [CC v3.1rx], la description des mesures de sécurité, ainsi que les tâches d'évaluation associées, sont requises pour l'application d'une démarche système cohérente.

b) Développement (ADV)

Cette classe ne s'applique qu'à la partie technique du système évalué. Aucune interprétation spécifique à une évaluation système n'est donc requise ici.

ADV_ARC

Les fournitures doivent décrire les mécanismes de sécurité mis en œuvre par le système.

ADV_FSP

Les fournitures doivent présenter les spécifications sécuritaires du système pour les objectifs de la partie technique du système (description du « quoi »).

ADV_TDS

Les fournitures doivent présenter la décomposition de la partie technique du système TI en sous-systèmes, conformément au niveau retenu, ainsi que les interfaces entre ces sous-systèmes (description du « comment »).

Les sous-systèmes peuvent correspondre aux différents produits intégrés au système.

c) Guides (AGD: AGD_OPE, AGD_PRE)

La répartition dans les composants AGD_OPE et AGD_PRE des guides identifiés ci-dessous doit être réalisée au cas par cas selon les particularités du système.

Par ailleurs, l'évaluateur doit appliquer les critères de AGD à tous les guides spécifiques à une évaluation système identifiés dans la présente note (voir l'Annexe B).

Guides destinés aux clients du système

Relativement à la partie technique du système, ces guides doivent décrire les actions des clients du système cible de l'évaluation nécessaires pour permettre la mise en route du système et/ou l'intégration des sites de ce client au système (par exemple, guide d'installation et de configuration des équipements sous responsabilité client).

Pour la partie non technique du système, ces guides doivent indiquer les mesures de sécurité auxquelles les clients doivent se conformer (par exemple, sous la forme de procédures de sécurité physique des sites clients).

Guides destinés aux développeurs du système

Ces guides doivent décrire les procédures d'administration (initialisation et maintenance) du système évalué, ainsi que les configurations évaluées de chacun des équipements composant la TOE.

Ces guides peuvent également décrire les procédures à appliquer pour permettre les évolutions du dimensionnement de ce système, le degré de liberté relatif à ces évolutions doit y être précisé, et sera évalué. Les évolutions adressées ici ne concernent que celles liées au dimensionnement, par exemple, ajout de nouveaux exemplaires d'équipements conformes à ceux identifiés dans la fiche de versions du système (cf. ALC_CMS et ALC_CMC). Ces évolutions ne doivent pas être de nature à modifier l'architecture du système décrite par ADV_ARC (par exemple, les redondances d'équipements imposées par la sécurité et/ou la sûreté de fonctionnement du système font partie de l'architecture système).

Pour la partie non technique du système, les guides doivent indiquer les mesures de sécurité auxquelles les sites de déploiement du système gérés par le développeur doivent se conformer (par exemple, sous la forme de procédures de sécurité physique des sites développeurs).

L'évaluateur doit vérifier que les mesures de sécurité des sites décrites dans les guides répondent correctement aux exigences support décrites dans la cible de sécurité.

L'ensemble des guides décrivant le contexte d'exploitation sera identifié dans le rapport de certification pour permettre la vérification, tant par l'utilisateur final, que par le développeur du système, de la mise en place du contexte de sécurité global tel que défini dans la cible de sécurité. Cette vérification pourrait être réalisée par un audit de conformité du type ISO27001/ISO17799/BS7799.

d) Cycle de vie (ALC)

ALC_CMC, ALC_CMS

Certaines de ces tâches sont menées sur la liste de configuration comme pour une évaluation de produit. Toutefois, le système pouvant évoluer, une fiche de versions doit également être fournie par le développeur. Cette fiche de versions doit identifier tous les différents types d'équipements intégrés (matériels) associés à toutes les différentes versions de logiciels déployées sur le système (versions des produits logiciels). Il n'est pas imposé que cette fiche de versions dénombre les équipements et logiciels déployés (i.e. le certificat restera valable même si la taille du système évolue). L'étiquetage de la cible d'évaluation est interprété comme étant cette fiche de versions (qui permet d'identifier la version évaluée du système) associée aux guides définissant les évolutions autorisées du système. C'est pourquoi cette fiche est toujours requise, quels que soient les composants d'assurance retenus par le commanditaire de l'évaluation.

Il est à noter qu'une correspondance cohérente entre la liste de configuration, les niveaux de représentation ADV et la fiche de versions est essentielle pour l'évaluation.

ALC_DEL

Les procédures de livraison du système à un client (livraison de l'accès au système) doivent décrire le processus de livraison des documents identifiés par AGD_OPE et les modalités d'application des guides AGD_PRE. Les procédures de livraison des équipements doivent également être décrites si ces derniers sont sous responsabilité client.

ALC_FLR

Les procédures de maintenance opérationnelle du système doivent décrire les modalités de déploiement des correctifs identifiés sur les composants techniques du système et les modalités d'évolution des mesures de sécurité physique des différents sites.

Le développeur doit également décrire le processus permettant à ces clients de le notifier en cas d'identification d'anomalies de sécurité, ainsi que le processus de traitement de ces anomalies.

e) Tests (ATE)

Cette classe ne s'applique qu'à la partie technique du système évalué.

ATE_COV, ATE_FUN

Ces tests sont réalisés en regard de ADV_FSP (les différents produits intégrés sont testés ensemble afin d'étudier leur collaboration). Les fournitures développeur doivent décrire l'environnement de test mis en œuvre et le CESTI doit se prononcer sur la représentativité de cette plate-forme (la fiche de versions et la liste de configuration du système auront donc dû être fournies précédemment). Des tests menés sur une plate-forme jugée non représentative pourront être rejetés par le CESTI.

ATE_IND

Ces tests sont également réalisés en regard de ADV_FSP. Une plate-forme de tests devra être mise à disposition du CESTI par le développeur pour que celui-ci puisse réaliser ses propres tests. Si cette plate-forme n'a pas été étudiée précédemment, le CESTI doit se prononcer sur sa représentativité. Une plate-forme jugée non représentative pourra être rejetée par le CESTI. Le développeur aura donc tout intérêt à fournir, en amont au déroulement de cette tâche, la description de cette plate-forme.

f) Vulnérabilités (AVA_VAN)

Les tests réalisés au titre de cette tâche d'évaluation ne s'appliquent qu'à la partie technique du système, mais l'exploitabilité des vulnérabilités techniques identifiées sera déterminée en regard des mesures de sécurité telles qu'évaluées dans AGD, en particulier celles décrivant plus avant les exigences de support décrites dans la cible.

Une plate-forme de test devra être mise à disposition du CESTI par le développeur pour réaliser ces tests. Si cette plate-forme n'a pas été étudiée précédemment, le CESTI doit se prononcer sur sa représentativité. Une plateforme jugée non représentative pourra être rejetée par le CESTI.

Annexe A

Correspondance pour les CC v2.x

La présente note est également applicable aux précédentes versions des CC. Seules des références à la version 3.1 des CC [CC v3.1rx] ont été exposées précédemment pour ne pas alourdir inutilement ce document.

Le tableau suivant précise comment appliquer cette note (essentiellement son chapitre 4.3) dans le cadre d'évaluation selon les [CC v2.x].

Paragraphes de la note	**Composants CC v3.1**	**Composants CC v2.x**
6.2.a	ASE_*	ASE_*
6.2.b	ADV_ARC	AVA_VLA
	ADV_FSP	ADV_FSP
	ADV_TDS	ADV_HLD
6.2.c	AGD_OPE	AGD_USR, AGD_ADM, AVA_MSU
	AGD_PRE	ADO_IGS, ADO_DEL AVA_MSU
6.2.d	ALC_CMC	ACM_CAP, ADO_IGS
	ALC_CMS	ACM_CAP
	ALC_DEL	ADO_DEL
	ALC_FLR	ALC_FLR
6.2.e	ATE_COV	ATE_COV
	ATE_FUN	ATE_FUN
	ATE_IND	ATE_IND
6.2.f	AVA_VAN	AVA_VLA

Annexe B

Quelques exemples de fournitures spécifiques à une évaluation système

Comme cela a été présenté précédemment, des fournitures spécifiques peuvent être produites dans le cadre d'une évaluation système.

Ces fournitures correspondent la plupart du temps à des guides. La nécessité d'obtenir ces guides dépend essentiellement du commanditaire du système (i.e. le client) et du périmètre qu'il a défini dans son cahier des charges. Ce cahier des charges doit également définir les responsabilités de chacune des parties. La cible de sécurité reflétera ce partage des responsabilités en déclinant les exigences non TI sur l'environnement en exigences support développeur ou exigences support client.

Cette étape préalable à l'évaluation sera toujours supposée réalisée dès que le processus d'évaluation aura été enclenché. En effet, la cible de sécurité présente le compromis qui a été établi entre commanditaire et développeur à l'issue de la contractualisation.

Le tableau suivant fournit quelques exemples de guides, relatifs à une évaluation système, non explicitement identifiés dans les critères communs. Tous ces guides sont évalués au regard de la classe AGD. L'évaluateur doit plus particulièrement s'assurer que :

- ces guides sont suffisants (ils couvrent, de façon pertinente, tous les aspects des exigences support identifiées dans la cible de sécurité) ;
- ces guides sont cohérents entre eux (ces guides ne contiennent pas de recommandations contradictoires).

	Partie TI	**Partie non TI**
AGD_OPE	• Guide d'initialisation du système (si l'initialisation - ou une partie de l'initialisation - est de responsabilité client) • Guide d'intégration d'un nouvel équipement (si le client y est autorisé) • …	• Mesures de sécurité physiques des sites clients (si la protection de ces sites est de responsabilité client) • Mesures de sécurité organisationnelles des sites clients • Support de formation des utilisateurs • …
AGD_PRE	• Guide de déploiement du système • Guide d'évolution du dimensionnement du système (si de telles évolutions sont prévues) • Procédures d'administration des équipements (ces procédures doivent être obligatoirement fournies, elles doivent décrire la configuration de chacun des types d'équipements si cette configuration n'est pas automatisée) • …	• Mesures de sécurité physiques des sites développeurs • Mesures de sécurité organisationnelles des sites développeurs • Support de formation des administrateurs • …