PREMIER MINISTRE

Secrétariat général
de la défense
nationale

Direction centrale de la sécurité des systèmes d'information

Paris, le 3 NOV 2005

3090/SGDN/DCSSI/SDR
Référence : NOTE/02.2

NOTE D'APPLICATION

VISITE DE L'ENVIRONNEMENT DE DÉVELOPPEMENT

Objet : Visite de l'environnement de développement
Application : A compter du 24 mars 2004
Diffusion : Publique

Vérifié par	Validé par Le sous-directeur "Régulation"	Vu l'avis du comité directeur Approuvé par Le Directeur central de la sécurité des systèmes d'information
Le responsable qualité [ORIGINAL SIGNE] *Le chef du centre de certification* [ORIGINAL SIGNE]	[ORIGINAL SIGNE]	[ORIGINAL SIGNE]

Suivi des modifications

Révision	Date	Modifications
1	23/03/04	Création
2	20/09/05	Changement de diffusion de “interne schéma” à “publique”

TABLE DES MATIERES

1. Présentation

1.1. Objet de la note

Dans le cadre d'une évaluation selon les Critères Communs (CC), certains critères précisent des exigences sur l'environnement de développement du produit en évaluation. La vérification de ces exigences par l'évaluateur peut conduire à une vérification de leur application par une visite sur le site de développement.

Cette note a pour objet de spécifier l'organisation d'une visite sur le site de développement.

1.2. Références

- Common Criteria for Information Technology Security Evaluation : ci-après « CC »
  - Part 1 : Introduction and general model, version 2.1, août 1999
  - Part 2 : Security functional requirements, version 2.1, août 1999
  - Part 3 : Security assurance requirements, version 2.1, août 1999
- Common Methodology for Information Technology Security Evaluation : ci-après « CEM »
  - Part 1 : Introduction and general model, version 0.6, janvier 1999
  - Part 2 : Evaluation Methodology, version 1.0, août 1999

1.3. Composants d'assurance pouvant nécessiter une visite

La CEM indique que la vérification des composants suivants peut être réalisée par une visite sur site :

- ACM_AUT.1 – Évaluation de l'automatisation du système de gestion de configuration – *Evaluation of CM automation*

  ACM_AUT.1-2 *The evaluator shall exercise the automated access control measures to determine whether they can be bypassed by an authorised role or user. This determination need only comprise a few basic tests.*

  ACM_AUT.1-7 *The evaluator looks for evidence that the tools and procedures are in use.*

- ACM_CAP.n (n = 3,4) – Évaluation des capacité du système de gestion de configuration – *CM capabilities*

  ACM_CAP.3-11 (4-12) *The evaluator shall examine the evidence to determine that the CM system is being used as it is described in the CM plan.*

- ADO_DEL.n (n = 1,2) – Évaluation des procédures de livraison – *Delivery*

  ADO_DEL.1-3 (2-5) *The evaluator shall examine aspects of the delivery process to determine that the delivery procedures are used.*

- ALC_DVS.1 – Sécurité de l'environnement de développement – Development security

  ALC_DVS.1-4 *The evaluator shall examine the development security documentation and associated evidence to determine that the security measures are being applied.*

La CEM ne couvrant pas les composants d'assurance au-delà de ceux compris dans EAL4, les composants hiérarchiquement supérieurs peuvent identifier d'autres éléments à vérifier lors de la visite.

1.4. Organisation du document

Les chapitres suivants présentent la démarche d'évaluation liée à la visite de ou des environnements de développement :

1. déterminer les sites à visiter ;
2. préparer la visite ;
3. effectuer la visite ;

4. émettre les conclusions de la visite ;
5. utiliser les résultats de la visite dans l'évaluation.

2. Sites nécessitant une visite

Pour chaque évaluation qui inclut les composants d'assurance référencés ci-dessus, la nécessité d'une visite sur le ou les sites de développements concernés sera déterminée de la manière suivante.

1. Identification des sites impactés par le développement du produit.

   L'évaluateur, à partir des informations sur le cycle de vie du produit (fourniture ALC_LCD), identifie tous les sites intervenant dans le développement et la production du produit évalué. En fonction des composants d'assurance de l'évaluation, il détermine les éléments à vérifier sur chaque site.

2. Discussion sur la nécessité d'une visite

   Pour chaque site, en fonction des éléments de preuve disponibles et d'autres éléments sur les sites concernés, il sera discuté de la nécessité d'y effectuer une visite. Cette discussion sera faite par le développeur avec le centre d'évaluation. (cf §1813 de la [CEM])

3. Liste des sites à visiter

   Au vu des arguments avancés, le certificateur décidera des visites à effectuer. La liste des sites pour lesquels une visite est effectuée sera communiquée au comité de pilotage.

Il est important que cette discussion soit faite suffisamment tôt dans le déroulement du projet, de préférence avant la réunion de démarrage de la certification.

3. Préparation de la visite

Pour chaque site identifié, une visite est organisée par le centre d'évaluation.

3.1. Tâches d'évaluation préalables

La visite sur site ne remplace pas l'analyse des documents et des éléments de preuve prévue dans l'évaluation mais a pour but de compléter ces informations et vérifier qu'ils correspondent à la réalité. Il est donc indispensable que, préalablement à la visite, l'évaluation des documents correspondants soit effectuée.

De manière pratique, l'évaluation des tâches considérées (ACM_AUT, ACM_CAP, ADO_DEL et ALC_DVS) doivent être réalisées avant le déroulement de la visite et pour chacune de ces tâches le seul élément empêchant l'émission d'un verdict "réussite" doit être l'attente des résultats de la visite (work-units de la CEM identifiées au §1.3).

3.2. Programme de visite

Pour chaque site, un programme de visite est proposé par le centre d'évaluation. Les éléments à vérifier pour chaque tâche sont décrits en Annexe A. Les informations qui doivent figurer dans le programme de visite sont décrites en Annexe B. Ce programme de visite est soumis à l'approbation du comité de pilotage.

3.3. Participation du certificateur

Le certificateur qui supervise l'évaluation se réserve le droit de participer à tout ou partie de la visite.

3.4. Méthodologie d'évaluation

Le centre d'évaluation doit disposer d'une méthodologie pour vérifier tous les éléments à vérifier décrits en Annexe A.

Cette méthodologie peut être adaptée aux particularités de chaque évaluation.

4. Déroulement de la visite

La visite se déroule selon le programme de visite approuvé.

4.1. Réunion de démarrage de la visite

La réunion de démarrage de la visite, outre les points fixés à l'ordre du jour, permet de fixer les créneaux horaires des différents éléments à vérifier et des personnes à rencontrer, afin d'être sûr de leurs disponibilités.

4.2. Vérification des éléments de preuve

L'évaluateur déroule la méthodologie de visite pour couvrir tous les éléments identifiés dans le programme de visite.

La vérification des éléments de preuve se fait de la manière la plus appropriée selon le contexte : interview du personnel, vérification d'enregistrements, démonstration d'opérations…

L'évaluateur veille à se limiter aux seuls aspects concernés par le produit en évaluation. Dans le cas où des éléments de preuve n'existent pas encore pour le produit concerné, des éléments pourront être vérifiés sur des projets analogues.

Si l'évaluateur détecte des problèmes, il émet des fiches de deux types : Fiche de remarque, Fiche de non-conformité. Les informations présentées par les fiches sont décrites dans l'Annexe C.

Pour chaque fiche, l'évaluateur détaille les éléments par rapport auxquels il fait ses commentaires et l'impact potentiel sur l'évaluation.

4.2.1. Fiches de remarque

Une fiche de remarque est émise si un élément, bien que répondant aux exigences, mériterait d'être amélioré.

Les fiches de remarques ne sont pas bloquantes pour l'évaluation, cependant certaines fiches de remarques peuvent soulever des problèmes qui pourraient être considérés comme bloquant dans le cadre d'une nouvelle évaluation.

4.2.2. Fiches de non-conformité

Une fiche de non-conformité est émise si un élément vérifié ne répond pas aux critères d'évaluation.

Afin d'obtenir un verdict "réussite" à la tâche associée, le développeur doit prévoir et mettre en place des actions correctives.

4.3. Conclusion de la visite

Lors de la réunion de conclusion de la visite, l'évaluateur fait le bilan des éléments vérifiés et livre au développeur les fiches de non-conformité et de remarque.

Le développeur concerné par la visite doit accepter ou non les fiches. Dans le cas où une fiche n'est pas acceptée, le litige sera traité par le certificateur après avis du comité de pilotage de l'évaluation.

Le développeur soumet les actions et les délais prévus pour la correction à l'évaluateur qui les accepte ou non. L'évaluateur spécifie également les éléments de preuve nécessaires à la vérification de la mise en œuvre de l'action corrective (procédure, trace d'audit, facture, visite complémentaire…).

Les fiches sont fermées lorsque la vérification de la mise en œuvre de l'action corrective a été réalisée.

Dans certains cas, l'évaluateur peut émettre un verdict réussite pour la tâche considérée même si la fiche n'est pas fermée. Cependant, les fiches non fermées seront systématiquement vérifiées lors de la maintenance associée au certificat ou d'une autre visite sur le site.

5. Rapport de visite

Pour chaque site un rapport de visite est rédigé par l'évaluateur.

Ce rapport retrace le déroulement général de la visite. Il permet de justifier les conclusions de la visite en décrivant pour chacun des éléments concernés ce qui a été vérifié et en quoi cela est satisfaisant.

Le rapport donne les conclusions de la visite et inclus les fiches émises.

Le rapport est émis lorsque les actions correctives associées à chaque fiche ont été approuvées par l'évaluateur.

Les éléments qui doivent apparaître dans un rapport de visite sont décrits en Annexe D.

Le rapport dédié à chaque visite doit permettre sa réutilisation pour des visites ultérieures.

6. Impact pour l'évaluation du produit

Les rapports de fin de tâche de chaque composant d'assurance ayant nécessité la visite référenceront le rapport de visite.

Annexe A Éléments à vérifier

a. Éléments à vérifier pour ACM_AUT.1 :

- ✓ **vérification de la gestion des droits d'accès pour le système de CM**
- ✓ **tentatives de contournement du contrôle d'accès**
- ✓ **vérification des éléments de preuve de l'utilisation du système de CM**
  - o **génération automatique de la TOE**
  - o **génération de la TOE avec tous les composants implémentant la TSP**

b. Éléments à vérifier pour ACM_AUT.2 :

- ✓ vérification de la gestion des droits d'accès pour le système de CM
- ✓ tentatives de contournement du contrôle d'accès
- ✓ vérification des éléments de preuve de l'utilisation du système de CM
  - o génération automatique de la TOE
  - o génération de la TOE avec tous les composants implémentant la TSP
  - o **identification des changements entre 2 versions**
  - o **identification de tous les éléments impactés par la modification d'un item géré en configuration**

c. Éléments à vérifier pour ACM_CAP.3 :

- ✓ **vérification des éléments de preuve de l'utilisation du système de CM**
  - o **lien entre les labels de la TOE et la documentation**
  - o **impact des opérations pendant le développement dans le système de CM**
  - o **rôles autorisés à faire les opérations**
  - o **éléments de preuves générés par le système de CM**
- ✓ **vérification de la conformité des éléments identifiés par l'outil avec le plan de CM**
- ✓ **interview du personnel pour vérifier que le système de CM est effectivement utilisé et que les procédures de CM sont appliquées**

d. Éléments à vérifier pour ACM_CAP.4 :

- ✓ vérification des éléments de preuve de l'utilisation du système de CM
  - o lien entre les labels de la TOE et la documentation
  - o impact des opérations pendant le développement dans le système de CM
  - o rôles autorisés à faire les opérations
  - o éléments de preuves générés par le système de CM
  - o **génération de la TOE**
  - o **gestion des modifications ou créations de nouveaux items dans le système de CM**
- ✓ vérification de la conformité des éléments identifiés par l'outil avec le plan de CM
- ✓ interview du personnel pour vérifier que le système de CM est effectivement utilisé et que les procédures de CM sont appliquées

e. Éléments à vérifier pour ACM_CAP.5 :

- ✓ vérification des éléments de preuve de l'utilisation du système de CM
  - o lien entre les labels de la TOE et la documentation
  - o impact des opérations pendant le développement dans le système de CM
  - o rôles autorisés à faire les opérations
  - o éléments de preuves générés par le système de CM
  - o génération de la TOE
  - o gestion des modification ou création de nouveaux items dans le système de CM
  - o **vérification des traces d'audit des modification de la TOE**
  - o **identification des master copies**
- ✓ vérification de la conformité des éléments identifiés par l'outil avec le plan de CM
- ✓ interview du personnel pour vérifier que le système de CM est effectivement utilisé et que les procédures de CM sont appliquées
- ✓ **vérification des éléments de preuve de l'utilisation de la procédure d'intégration**
  - o **différentiation des rôles**

f. Élément à vérifier pour ADO_DEL.1 :

- ✓ **vérification de l'application de la procédure de livraison**

g. Élément à vérifier pour ADO_DEL.2 :

- ✓ vérification de l'application de la procédure de livraison
- ✓ **vérification des éléments de preuve pour la détection des modification**
- ✓ **vérification des éléments de preuve contre l'usurpation de l'identité du développeur**

h. Élément à vérifier pour ADO_DEL.3 :

- ✓ vérification de l'application de la procédure de livraison
- ✓ **vérification des éléments de preuve pour la prévention des modification**
- ✓ vérification des éléments de preuve contre l'usurpation de l'identité du développeur

i. Éléments à vérifier pour ALC_DVS.1 :

- ✓ **vérification de l'existence de moyens de protection des informations de conception de la TOE et des échantillons**
  - o **protections physiques**
    - ◆ **sécurisation de la zone**
      - □ **alarmes**
      - □ **administration de la sécurité**
      - □ **personnel de sécurité**
    - ◆ **contrôle d'accès**
      - □ **gestion des droits (initialisation, vérification, révocation…)**
      - □ **accès restreint à l'équipe du projet**
      - □ **gestion des clés, codes d'accès, badges…**
    - ◆ **stockages physique sécurisés**
      - □ **gestion des codes d'accès (initialisation, renouvellement…)**
    - ◆ **sécurité physique des moyens informatiques**

- **protections informatiques**
  - **réseau sécurisé**
    - **cloisonnement du réseau**
    - **administration du réseau**
  - **contrôle d'accès**
    - **moyens d'authentification**
    - **gestion des droits (affectation, révocation, vérification…)**
    - **gestion des mots de passe (renouvellement, complexité…)**
  - **sauvegardes**
  - **moyens de stockages**
- **protection organisationnelle**
  - **gestion du transfert des informations**
  - **gestion du personnel de sécurité**
  - **identification du personnel de développement**
  - **fiabilité du personnel**
    - **établissement de la confiance dans les personnes**
    - **sensibilisation à la sécurité**
  - **gestion du personnel extérieur au projet (visiteurs, nettoyage, maintenance…)**
  - **gestion et maintenance des moyens informatiques**
  - **gestion et maintenance des moyens de sécurité physique**

- ✓ **conformité des moyens de protection observés avec les procédures**
- ✓ **vérification d'éléments de preuve de l'application des procédures**
- ✓ **examen des éléments qui prouvent l'application des procédures**
- ✓ **interview du personnel pour vérifier leur connaissance de la politique de sécurité, des procédures et de leur propre responsabilité**

j. Éléments à vérifier pour ALC_DVS.2 :

- ✓ vérification de l'existence de moyens de protection des informations de conception de la TOE et des échantillons
  - protections physiques
    - sécurisation de la zone
      - alarmes
      - administration de la sécurité
      - personnel de sécurité
    - contrôle d'accès
      - gestion des droits (initialisation, vérification, révocation…)
      - accès restreint à l'équipe du projet
      - gestion des clés, codes d'accès, badges…
    - stockages physique sécurisés
      - gestion des codes d'accès (initialisation, renouvellement…)
    - sécurité physique des moyens informatiques
  - protections informatiques
    - réseau sécurisé
      - cloisonnement du réseau

        - administration du réseau
    - contrôle d'accès
        - moyens d'authentification
        - gestion des droits (affectation, révocation, vérification…)
        - gestion des mots de passe (renouvellement, complexité…)
    - sauvegardes
    - moyens de stockages
- protection organisationnelle
    - gestion du transfert des informations
    - gestion du personnel de sécurité
    - identification du personnel de développement
    - fiabilité du personnel
        - établissement de la confiance dans les personnes
        - sensibilisation à la sécurité
    - gestion du personnel extérieur au projet (visiteurs, nettoyage, maintenance…)
    - gestion et maintenance des moyens informatiques
    - gestion et maintenance des moyens de sécurité physique

- ✓ conformité des moyens de protection observés avec les procédures
- ✓ vérification d'éléments de preuve de l'application des procédures
- ✓ examen des éléments qui prouvent l'application des procédures
- ✓ interview du personnel pour vérifier leur connaissance de la politique de sécurité, des procédures et de leur propre responsabilité
- ✓ **vérification de la cohérence des différentes mesures de sécurité et de leur adéquation avec le niveau des informations à protéger**

Annexe B Programme de visite

a. Introduction du programme de visite :

- Nom du projet
- Tâches d'évaluation concernées
- Date de la visite
- Nom et adresse géographique du site concerné
- Nom de l'évaluateur effectuant la visite

b. Ordre du jour de la visite :

- Réunion de démarrage de la visite avec l'équipe de visite (évaluateur et certificateur) et les personnes rencontrées
    - Présentation de l'équipe de visite
    - Présentation des objectifs de la visite (spécialement pour le personnel qui ne connaît pas directement les exigences de l'évaluation)
    - Présentation des personnes rencontrées
    - Présentation du site
- Pour chaque élément à vérifier (en fonction des procédures évaluées)
    - Forme de la visite (vérification sur poste de travail, interview…)
    - Personnels requis pour des interviews
- Débriefing de l'équipe de visite.
- Réunion de clôture de la visite avec les l'équipe de visite et les personnes rencontrées
    - Conclusions de la visite
    - Transmission des éventuelles fiches de remarque ou d'anomalie

Annexe C Fiche de remarque / non-conformité

a. Identification de la fiche :

- Type de fiche (Remarque / Non-conformité)
- Référence de la fiche
- Nom du projet
- Tâche d'évaluation concernée
- Date de la visite
- Nom du site concerné
- Nom de l'évaluateur

b. Description de l'anomalie

- Description détaillée de l'anomalie

c. Accord du développeur

- Accord ou non du développeur
- Argument en cas de désaccord
- Date
- Nom du développeur

d. Proposition d'action corrective

- Description de l'action corrective proposée
- Délai de mise en œuvre
- Date
- Nom du développeur

e. Validation de l'action corrective

- Validation de la proposition par l'évaluateur
- Modalité de vérification envisagée
- Date
- Nom de l'évaluateur

f. Fermeture de la fiche

- Référence des éléments de preuve de l'action corrective (référence document, visite…)
- Fermeture de la fiche avec verdict de l'évaluateur
- Date
- Nom de l'évaluateur

Annexe D Rapport de visite

a. Introduction du rapport de visite :

- Nom du projet
- Tâches d'évaluation concernées
- Date de la visite
- Nom et adresse géographique du site concerné
- Nom de l'évaluateur
- Référence du programme de visite
- Référence de la méthodologie de visite

b. Déroulement de la visite

- Pour chaque élément à vérifier
  - description des éléments vérifiés
  - identification des rôles du personnel rencontré
  - verdict de l'évaluateur
  - référence éventuelle des fiches émises

c. Conclusion de la visite

- Récapitulatif des éléments visités
- Verdict de l'évaluateur

d. Fiches en annexes