PREMIÈRE MINISTRE

Liberté
Égalité
Fraternité

Agence nationale de la sécurité des systèmes d'information

Secrétariat général de la défense et de la sécurité nationale

Paris, le 23/11/2023

N° 2027 **/ANSSI/SDE/PSS/CCN**

Référence **: ANSSI-CC-NOTE-02_v6.1**

NOTE D'APPLICATION

VISITE DE L'ENVIRONNEMENT DE DEVELOPPEMENT

Application **:** Dès son approbation.

Diffusion **:** Publique

Le sous-directeur « Expertise »
de l'Agence nationale de la sécurité
des systèmes d'information

Renaud LABELLE

[ORIGINAL SIGNE]

SÉCURITÉ CERTIFICATION

SUIVI DES MODIFICATIONS

Version	Date	Modifications
1	23/03/04	Création
2	20/09/05	Changement de diffusion de "interne schéma" à "publique"
3	16/12/2010	– prise en compte des CC v3.1 ; – introduction d'un chapitre relatif à la réutilisation des résultats ; – modification du chapitre 6 relatif à l'impact pour l'évaluation ; – introduction d'ALC_FLR dans le contour de l'audit
4	05/01/2015	Prise en compte du référentiel MSSR
5	12/04/2016	Relatif à la participation obligatoire des certificateurs du centre de certification
6	16/04/2021	– Ajout de la CEM en référence ; – Précision des tâches d'évaluation préalables (chapitre 3.1) ; – Ajout du délai concernant le programme de visite (chapitre 3.2) ; – Référence à la MSSR dans la méthodologie d'évaluation (chapitre 3.4) ; – Modification des chapitres 5, 6 réorganisés en sous-chapitres : Traitement des remarques et non-conformités & Rédaction du rapport de visite pour le chapitre 5, et Durée de validité (modifiée) & Utilisation dans le cadre de la certification d'un produit pour le chapitre 6 ; – Modification de la durée de validité des résultats de visite (chapitre 6.1)
6.1	17/11/2023	– Mise à jour de l'adresse du site du SOG-IS dans la description des références [MSSR] et [Checklist], et clarification usage de l'ANNEXE B.

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

Cette note est également soumise pour avis lors de chaque modification majeure conformément au manuel qualité du centre de certification. Les évaluations mineures ne sont pas soumises au comité directeur de la certification.

La présente note est disponible en ligne sur le site institutionnel de l'ANSSI (www.cyber.gouv.fr).

TABLE DES MATIERES

1 Présentation

1.1 Objet de la note

Dans le cadre d'une évaluation selon les Critères Communs (CC), soit de produits (voir [CC-CER-P-01]), soit de composants ALC génériques (voir [CC-SITE-P-02]), certains composants d'assurance fixent des exigences sur l'environnement de développement du produit en évaluation. La vérification de l'application de ces exigences peut nécessiter une visite du site de développement.

Cette note a pour objet de préciser les composants d'assurance nécessitant une visite de site et d'en spécifier l'organisation.

1.2 Organisation du document

Les chapitres 2 à 6 de la présente note présentent les différentes étapes de l'organisation de la visite du ou des environnements de développement :

- déterminer les sites à visiter ;
- préparer la visite ;
- effectuer la visite ;
- émettre les conclusions de la visite ;
- utiliser les résultats de la visite dans les évaluations.

L'ANNEXE B liste les composants d'assurance nécessitant une visite de site dans le cadre des évaluations du schéma français de certification.

2 Sites nécessitant une visite

Sur la base des informations disponibles dans le dossier d'évaluation [CC-CER-F-01] incluant des tâches ALC, le comité de pilotage de l'évaluation identifie la liste des sites nécessitant une visite.

Si, au cours du processus d'évaluation d'un produit ou d'une évaluation de composants ALC génériques, la visite de nouveaux sites est estimée nécessaire, cette liste est réexaminée par le comité de pilotage.

3 Préparation de la visite

Le centre d'évaluation doit préparer comme suit chacune des visites de site prévues.

3.1 Tâches d'évaluation préalables

La visite sur site a pour but de compléter l'analyse des documents et des éléments de preuve prévus dans l'évaluation, en vérifiant que ces informations correspondent à la réalité. Il est donc indispensable que, préalablement à la visite, l'évaluation des documents correspondants soit effectuée.

En particulier, quand [MSSR] est utilisé, la [Checklist] doit être pré-remplie par le développeur sur les parties qui le concernent et envoyée au CESTI et à l'ANSSI. La partie revue documentaire de la [Checklist] doit être réalisée par le CESTI avant la visite.

De manière pratique, la visite ne doit être organisée qu'à la suite de l'édition d'un rapport intermédiaire, relatif aux *work-units* de la [CEM] des composants d'assurance de l'ANNEXE B, dont le seul élément empêchant l'émission d'un verdict « réussite » est l'attente des résultats de la visite.

3.2 Programme de visite

Pour chaque site, un programme de visite est préparé par le centre d'évaluation. Les éléments à vérifier pour chaque tâche sont décrits par la [CEM].

Les informations qui doivent figurer dans le programme de visite sont décrites en ANNEXE C. Ce programme de visite est soumis à l'approbation du comité de pilotage au minimum un mois avant la date de la visite.

3.3 Participation du certificateur

Le certificateur qui supervise l'évaluation ou, le cas échéant, celui qui supervise les visites de sites du développeur concerné, se réserve le droit d'indiquer la participation d'un ou plusieurs certificateurs à toute ou partie de la visite.

Le centre de certification participe systématiquement aux visites réalisées par les CESTI visant un premier agrément.

3.4 Méthodologie d'évaluation

Le centre d'évaluation doit disposer d'une méthodologie pour évaluer tous les éléments à vérifier décrits par la [CEM]. Lorsque la checklist [MSSR] est utilisée, la vérification et la complétude par rapport à cette checklist doit faire partie de cette méthodologie.

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 par le comité de pilotage.

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 la liste des personnes à rencontrer, afin d'être assuré de leur disponibilité.

4.2 Vérification des éléments de preuve

L'évaluateur déroule la méthodologie de visite pour 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, etc.

L'évaluateur veille à se limiter aux seuls aspects concernés par les évaluations Critères communs.

Lors de la visite, l'évaluateur peut être amené à émettre des fiches de deux types : fiche de remarque, fiche de non-conformité. L'ANNEXE D présente les informations minimales que ces fiches doivent fournir.

Sur chaque fiche, l'évaluateur détaille les éléments qui l'ont conduit à formuler ses commentaires et l'impact potentiel sur l'évaluation.

4.3 Fiches de remarque

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

Les fiches de remarque ne sont cependant pas bloquantes pour l'évaluation, le verdict des rapports correspondant peut être positionné à « réussite » sans que celles-ci ne soient closes (voir §5.1).

Les fiches de remarques non fermées seront systématiquement vérifiées à l'issue de la validité de l'audit de site.

4.4 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, une fiche de conformité doit être traitée et close (voir §5.1).

4.5 Conclusion de la visite

Lors de la réunion de conclusion de la visite, l'évaluateur fait le bilan des éléments vérifiés et communique au développeur les non-conformités et remarques éventuelles. Chaque non-conformité ou remarque est formalisée par le CESTI dans une fiche communiquée au développeur.

Le développeur 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.

5 Rapport de visite

5.1 Traitement des remarques et non-conformités

Pour traiter une fiche de remarque ou de non-conformité,

1. le développeur doit soumettre à l'évaluation un plan d'actions comprenant les actions correctives et les délais prévus pour la correction ;
2. le CESTI approuve la pertinence du plan d'action et spécifie les éléments de preuve nécessaires à la vérification de la mise en œuvre du plan d'actions (procédure, trace d'audit, facture, visite complémentaire, etc.).

Une fiche peut être close lorsque la mise en œuvre du plan d'actions a été vérifiée par le CESTI au travers des éléments de preuve mis à disposition par le développeur.

Cas particulier : non-conformité impactant la confidentialité du développement de produit

Si le développeur ne peut pas traiter une non-conformité dans le temps imparti à l'évaluation du site considéré (longue à mettre en place, trop coûteuse à résoudre, dépendante de facteurs extérieurs, etc.) et qu'uniquement la confidentialité du développement de produits est impactée, alors la fiche de non-conformité associée peut être close si le développeur décide que le *knowledge of the TOE* de ces produits soit positionné à zéro lors de leurs évaluations. Cette information devra apparaître dans le rapport de visite du CESTI.

5.2 Rédaction du 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 inclut les fiches émises.

Les éléments qui doivent apparaître dans un rapport de visite sont décrits en ANNEXE E.

6 Utilisation des résultats des visites

6.1 Durée de validité

Une fois le rapport d'audit validé par le centre, les résultats de visites peuvent en général être réutilisés jusqu'à un an après la visite du site.

Quand [MSSR] est utilisé, les résultats de visites validés par le centre, peuvent être réutilisés jusqu'à deux ans et demi après la visite du site.

6.2 Utilisation dans le cadre de la certification d'un produit

Les rapports de fin de tâche de chaque composant d'assurance ayant nécessité les visites, les rapports techniques intermédiaires (RTI) et le rapport technique d'évaluation (RTE), indiqueront les références des rapports de visite.

Le CESTI devra s'assurer, dans le cadre de l'évaluation, que le développement est réalisé selon les procédures auditées et avec les moyens (locaux, architecture du SI etc.) vus lors de la visite de site, ou, lorsque des modifications de ces derniers sont intervenues, des moyens au moins équivalents.

Le rapport de certification ne recense que les sites qui ont été effectivement audités pendant une évaluation ou les sites dont l'audit a été réutilisé.

Rappel sur l'impact des audits sur l'analyse de vulnérabilités :

> Les points accordés dans une cotation d'attaque pour le critère « *knowledge of the TOE* » dépendent du niveau de la protection assurée par le développeur, conformément au niveau ALC_DVS visé, pour les éléments qui pourraient être utilisés pour cette attaque.

6.3 « Réévaluation » d'un audit

Dans le cas où un site est à nouveau visité, la qualification des fiches de remarque émises précédemment doit être reconsidérée.

Si le développeur a mis en place des mesures correctives, le CESTI doit les vérifier. Suivant la nature des mesures, cette vérification peut être effectuée au travers d'une analyse documentaire, d'une visite ou les deux.

Si les remarques sont devenues bloquantes (exemple : évolution de l'état de l'art), les fiches associées deviennent des fiches de non-conformité.

ANNEXE A. Références

Référence	Document
[CC]	*Common Criteria for Information Technology Security Evaluation*, version en vigueur.
[CEM]	*Common Methodology for Information Technology Security Evaluation*, version en vigueur.
[Checklist]	*Checklist (corresponding to MSSR vx.x)*, version en vigueur disponible sur le site du SOG-IS (www.sogis.eu).
[MSSR]	*Minimum Site Security Requirement*, version en vigueur disponible sur le site du SOG-IS (www.sogis.eu).
[CC-CER-P-01]	Certification Critères communs de la sécurité offerte par les produits, les systèmes des technologies de l'information, les sites ou les profils de protection, référence ANSSI-CC-CER-P-01, version en vigueur.
[CC-SITE-P-02]	Evaluation de composants d'assurance ALC génériques, référence ANSSI-CC-SITE-P-02, version en vigueur.
[CC-CER-F-01]	Dossier d'évaluation, référence ANSSI-CC-CER-F-01, version en vigueur.

La plupart de ces documents peuvent être consultés et téléchargés depuis le site de l'ANSSI (www.cyber.gouv.fr).

ANNEXE B. Éléments à vérifier

Les composants d'assurance nécessitant une visite de site dans le cadre des évaluations du schéma français de certification sont listés dans cette annexe.

a. En CC v2.3

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

ACM_CAP.3, ACM_CAP.4 – Évaluation des capacités du système de gestion de configuration – *Evaluation of CM capabilities*

ADO_DEL.1, ADO_DEL.2 – Évaluation des procédures de livraison – *Evaluation of Delivery*

ALC_DVS.1 – Evaluation de la sécurité de l'environnement de développement – Evaluation of *Development security*

b. En CC v3.1

ALC_CMC.3, ALC_CMC.4, ALC_CMC.5 – Évaluation des capacités du système de gestion de configuration – *CM capabilities*

ALC_DEL.1 – Évaluation des procédures de livraison – *Delivery*

ALC_DVS.1, ALC_DVS.2 – Evaluation de la sécurité de l'environnement de développement – *Development security*

ALC_TAT.2, ALC_TAT.3 – Conformité avec les standards d'implémentations

c. ALC_FLR : procédures de correction des anomalies de sécurité

Le schéma français de certification impose que les procédures de correction des anomalies de sécurité (composants d'assurance ALC_FLR.1, ALC_FLR.2 et ALC_FLR.3) soient également auditées. En effet, seul l'audit permet de s'assurer que les moyens spécifiques, identifiés dans les fournitures associées à FLR, sont effectivement mis en œuvre par le développeur.

La partie de l'audit relative à ces composants sera réalisée, autant que possible, sur les corrections du produit en cours d'évaluation.

ANNEXE C. 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, et, si nécessaire, désignation des pièces concernées
- 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 l'équipe de visite et les personnes rencontrées
    - Conclusions de la visite
    - Transmission des éventuelles fiches de remarque ou de non-conformité

ANNEXE D. 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
- Eventuel lien vers une précédente fiche de remarque

b. Description de remarque / non-conformité

- Description détaillée de remarque / non-conformité comprenant **notamment une justification de la qualification en remarque / non-conformité**

c. Accord du développeur

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

d. Proposition de plan d'actions correctives

- Description des actions correctives proposées
- Délai de mise en œuvre
- Date
- Nom du développeur

e. Validation du plan d'action

- 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, etc.)
- Verdict de l'évaluateur
- Date
- Nom de l'évaluateur

ANNEXE E. Rapport de visite

a. Introduction

- Identification du rapport
- Nom du CESTI
- Nom du centre de certification
- Date de rapport
- Composition de l'équipe d'audit (évaluateurs et certificateurs)
- Nom et adresse du ou des site(s) visité(s)
- Date de la ou des visite(s)
- Identification de personnes rencontrées pendant les visites de sites
- Références aux CC et à la méthodologie utilisée
- Information des visites précédentes (si existantes) avec la référence à leur rapport de visite. En particulier, le statut des remarques ouvertes lors de la dernière visite
- Nom du projet
- Tâches d'évaluation concernées
- Programme de visite

b. Description de l'évaluation

- Description des activités auditées
- Liste des *work-units* de la classe d'assurance ALC évaluées pendant la visite de site
- Référence au rapport contenant les travaux documentaires préalables décrits au paragraphe 3.1 (ces éléments peuvent être directement décrits dans le rapport de visite)
- Référence à l'ensemble de la documentation du développeur (politiques et procédures) et la liste des outils (en particulier le système de gestion de la configuration)
- Référence à la [Checklist] complétée lors de l'évaluation
- 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
- Résultats de l'évaluation pour chaque *work-unit*
- Liste des remarques émises et de leur statut (comprenant le statut des remarques du dernier audit clôturées dans le cadre de cet audit)