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, April 12th, 2016

Reference: ANSSI-CC-NOTE-02/5.0.1EN

APPLICATION NOTE

DEVELOPMENT ENVIRONMENT VISIT

Application : From date of publication.

Circulation : Public.

COURTESY TRANSLATION

SÉCURITÉ CERTIFICATION

51 boulevard de La Tour-Maubourg - 75700 PARIS 07 SP

Version history

Versions	Date	Modifications
1	23/03/2004	Creation
2	20/09/2005	Change in distribution from "internal scheme" to "public"
3	16/12/2010	– Acknowledgement of the CC v3.1; – Introduction of a chapter relating to the reuse of results; – Modification of chapter 6 relating to the impact for the evaluation; – Introduction of ALC_FLR within the scope of the audit.
4	05/01/2015	Acknowledgement of the MSSR reference base
5	12/04/2016	Relating to the mandatory participation of the certification centre certifiers
5.0.1	05/10/2016	Update to fix translation mistakes.

Table of Contents

1. Presentation

1.1. Subject of the note

In the context of an evaluation according to the Common Criteria (CC), certain assurance components set requirements for the development environment of the product being evaluated. The evaluation may therefore require verification of these requirements with a site visit of the development site.

The purpose of this note is to specify the organisation of a site visit of the development site.

1.2. References

- [CC v2.3]: Common Criteria Parts 1-2-3 and [CEM]; Version 2.3; August 2005; Ref.: CCMB-2005-08-001 to 004.
- [CC v3.1]: Common Criteria Parts 1-2-3 and [CEM]; Version 3.1; Revision 4 Final; September 2012; Ref.: CCMB-2012-09-001 to 004.
- [MSSR]: Minimum Site Security Requirement; current version available on sogisportal.eu.

1.3. Document organisation

Chapters 2 to 6 of this note present the different steps in the organisation of the visit of the development environments:

- Determine the sites to be visited;
- Prepare the visit;
- Carry out the visit;
- Issue the conclusions of the visit;
- Use the results of the visit in the evaluations.

1.4. Assurance components requiring a visit

As the [CEM] does not cover all the assurance components, the components that are hierarchically superior to those listed below may require other verifications during the visit.

1.4.1. In CC v2.3

The [CEM] indicates that the following components must be verified with an on-site visit:

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

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

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

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

ACM_CAP.3-12, ACM_CAP.4-13 *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.1, ADO_DEL.2 – Évaluation des procédures de livraison – *Evaluation of Delivery*

ADO_DEL.1-2, ADO_DEL.2-4 *The evaluator shall examine aspects of the delivery process to determine that the delivery procedures are used*.

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

1.4.2. In CC v3.1

The [CEM] indicates that the following components must be verified with an on-site visit:

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

ALC_CMC.3-10, ALC_CMC.4-13, ALC_CMC.5-19: *The evaluator shall examine the evidence to determine that the CM system is being operated in accordance with the CM plan*

ALC_CMC.5-20 *The evaluator shall examine the production support procedures to determine that by following these procedures a TOE would be produced like that one provided by the developer for testing activities*

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

ALC_DEL.1-2: *The evaluator shall examine aspects of the delivery process to determine that the delivery procedures are used*

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

ALC_DVS.1-3, ALC_DVS.2-4: *The evaluator shall examine the development security documentation and associated evidence to determine that the security measures are being applied*

1.4.3. ALC_FLR: security anomaly correction procedures

The French certification scheme now requires the security anomaly correction procedures (ALC_FLR.1, ALC_FLR.2 and ALC_FLR.3 assurance components) to be also audited. In fact, only the audit guarantees that the specific resources, identified in the deliveries associated with FLR, are actually implemented by the developer.

As far as possible, the part of the audit relating to these components will be carried out on the corrections of the product being evaluated.

2. Sites requiring an visit

Based on the information available in the evaluation file, in the certification start-up meeting the evaluation steering committee identifies the list of sites requiring an visit.

If the visit of new sites is considered necessary during the evaluation process, this list is re-examined by the steering committee.

3. Preparation of the visit

The evaluation centre must prepare each site visit as follows.

3.1. Prior evaluation tasks

The purpose of the on-site visit is to complete the analysis of the evidence documents and elements specified in the evaluation by verifying that this information corresponds to reality. It is therefore mandatory that the corresponding documents are evaluated before the visit.

On a practical level, the visit may only be organised following the issue of reports relating to the *work units* of the [CEM] identified in §1.4, the only element of which preventing the issue of a "success" verdict is the pending results of the visit.

3.2. Visit programme

A visit programme is prepared for each site by the evaluation centre. The elements to be verified for each task are described in Appendix A 0. The information the visit programme must contain is described in Appendix B. This visit programme is submitted to the steering committee for approval.

3.3. Certifier's participation

The certifier who supervises the evaluation, or if need be, the one which supervises the site visits of the concerned developer, reserves the right to take part in all or part of the visit.

The certification centre systematically takes part in the visits carried out by the CESTI which is aiming at the first licensing.

The CESTI in charge of the audit informs the certifier of the date when the audit will be carried out at the latest a month before the given date.

3.4. Evaluation methodology

The evaluation centre must have a methodology to evaluate all the elements to be verified described in Appendix A.

This methodology may be adapted to the specifics of each evaluation.

4. Conduct of the visit

The visit is carried out according to the visit programme approved by the steering committee.

4.1. Visit start-up meeting

In addition to the points set in the agenda, the visit start-up meeting sets the time frames for the different elements to be verified and the list of people to be met in order to guarantee their availability.

4.2. Verification of the evidence elements

The evaluator rolls out the visit methodology for all the elements identified in the visit programme.

The evidence elements are verified in the most appropriate way according to the context: interviews with personnel, verification of records, demonstration of operations and so on.

The evaluator makes sure that they only verify the aspects concerned by the product being evaluated. If there are not yet any evidence elements for the product concerned, elements may be verified on similar projects.

If the evaluator detects any problems, they issue two types of file: a remark file and a non-conformity file. 0 Appendix C presents the minimum information these files must contain.

The evaluator details on each file the elements which led them to formulate their comments and the potential impact on the evaluation.

4.2.1. Remark files

A remark file is issued if an element needs to be improved, even if it meets the requirements.

However, these remark files do not block the evaluation (the corresponding report verdict may be set to "success").

4.2.2. Non-conformity files

A non-conformity file is issued if a verified element does not meet the evaluation criteria.

In order to obtain a "success" verdict for the associated task, the developer must provide for and put in place corrective actions during the evaluation in progress.

4.3. Conclusion of the visit

During the visit conclusion meeting, the evaluator draws up the list of elements verified and provides the developer with the non-conformity and remark files.

The developer concerned by the visit may choose to accept or reject the files. If a file is not accepted, the dispute will be dealt with by the certifier after taking the opinion of the evaluation's steering committee.

The developer submits the actions and deadlines planned for the correction to the evaluator, who accepts or rejects them. The evaluator specifies the evidence elements needed to verify that the corrective action is in place (procedure, audit trace, invoice, complementary visit and so on).

The files are closed when the implementation of the corrective action has been verified.

Depending on the evaluator's assessment, a "success" verdict for the task in question may be issued even if the file is not closed. However, the files which are not closed will always be verified during the maintenance associated with the certificate or during a later visit on the site.

5. Visit report

A visit report is drafted for each site by the evaluator.

This report outlines the general conduct of the visit. It is used to justify the conclusions of the visit by describing for each element concerned what was verified and how it is satisfactory.

The report provides the conclusions of the visit and includes the files issued.

The elements which a visit report must contain are described in Appendix D.

The visit report must be able to be re-used for later visits.

6. Using the visit results

The end of task reports for each assurance component which required the visits will indicate the visit report references.

The certification report only covers the sites which were actually audited during an evaluation or the sites whose audit was re-used.

Reminder of the impact of the audits on the vulnerability analysis:

> The points awarded in an attack rating for the "*knowledge of the TOE*" criterion depend on the level of protection provided by the developer, in accordance with the targeted ALC_DVS level, for the elements which might be used for this attack.

The audit reports may be re-used in a later evaluation up to one year after the site visit. To do so, the CESTI must ensure that the same resources (premises, IT equipment, etc.) are used for the development.

One exception to the above rule: the period for re-using results from visits carried out according to [MSSR] may be extended to two years if no remarks are made in this report or if the centre's analysis of the remarks and actions specified by the audited party enables this exceptionally.

If audit results are re-used, the qualification of the remark files issued during the first audit must be reconsidered. In general, if the remarks have not always been taken into account, the remark files become non-conformity files. If the CESTI does not carry out the visit, they must ensure by documentary verification that the developer has put in place the suitable corrective measures.

APPENDIX A Elements to be verified

This appendix only deals with the cases in [CC v2.3].

For the [CC v3.1], see the transition guides between CC versions 2.3 and 3.1, published on the "www.commoncriteriaportal.org" website.

a. Elements to be verified for ACM_AUT.1:

- ✓ **verification of the access right management for the configuration management system**
- ✓ **verification of the inability to avoid the access control system**
- ✓ **verification of the evidence elements that the configuration management system has been used**
  - o **automatic TOE generation**
  - o **TOE generation with all the components that implement the TSP**

b. Elements to be verified for ACM_AUT.2:

- ✓ verification of the access right management for the configuration management system
- ✓ verification of the inability to avoid the access control system
- ✓ verification of the evidence elements that the configuration management system has been used
  - o automatic TOE generation
  - o TOE generation with all the components that implement the TSP
  - o **identification of changes between 2 versions**
  - o **identification of all the elements affected by the modification of an item managed in configuration**

c. Elements to be verified for ACM_CAP.3:

- ✓ **verification of the evidence elements that the configuration management system has been used**
  - o **link between the TOE labels and the documentation**
  - o **impact of the operations during development in the configuration management system**
  - o **roles authorised to carry out the operations**
  - o **evidence elements generated by the configuration management system**
- ✓ **verification of the conformity of the elements identified by the tool with the configuration management plan**
- ✓ **interview with personnel to verify that the configuration management system is actually used and that the configuration management procedures are applied**

d. Elements to be verified for ACM_CAP.4:

- ✓ verification of the evidence elements that the configuration management system has been used
  - o link between the TOE labels and the documentation
  - o impact of the operations during development in the configuration management system
  - o roles authorised to carry out the operations

- evidence elements generated by the configuration management system
- **TOE generation**
- **management of new item modifications or creations in the configuration management system**

✓ verification of the conformity of the elements identified by the tool with the configuration management plan

✓ interview with personnel to verify that the configuration management system is actually used and that the configuration management procedures are applied

e. Elements to be verified for ACM_CAP.5:

✓ verification of the evidence elements that the configuration management system has been used

- link between the TOE labels and the documentation
- impact of the operations during development in the configuration management system
- roles authorised to carry out the operations
- evidence elements generated by the configuration management system
- TOE generation
- management of new item modifications or creations in the configuration management system
- **verification of the TOE modification audit traces**
- **master copy identification**

✓ verification of the conformity of the elements identified by the tool with the configuration management plan

✓ interview with personnel to verify that the configuration management system is actually used and that the configuration management procedures are applied

✓ **verification of the evidence elements that the integration procedure has been used**

- **role differentiation**

f. Element to be verified for ADO_DEL.1:

✓ **verification that the delivery procedure is applied**

g. Element to be verified for ADO_DEL.2:

✓ verification that the delivery procedure is applied

✓ **verification of the evidence elements for the modification detection**

✓ **verification of the evidence elements against developer identity theft**

h. Element to be verified for ADO_DEL.3:

✓ verification that the delivery procedure is applied

✓ **verification of the evidence elements for modification prevention**

✓ verification of the evidence elements against developer identity theft

i. Elements to be verified for ALC_DVS.1:

- ✓ **verification that protection resources exist for the TOE design information and samples**
  - **physical protection**
    - **area security**
      - **alarms**
      - **security administration**
      - **security personnel**
    - **access control**
      - **rights management (initialisation, verification, revocation, etc.)**
      - **access restricted to the project team**
      - **key, access code, badge, etc. management**
    - **secured physical storage**
      - **access code management (initialisation, renewal, etc.)**
    - **physical IT resource security**
  - **electronic protection**
    - **secured network**
      - **network partitioning**
      - **network administration**
    - **access control**
      - **authentication resources**
      - **rights management (assignment, revocation, verification, etc.)**
      - **password management (renewal, complexity, etc.)**
    - **backup**
    - **storage resources**
  - **organisational protection**
    - **information transfer management**
    - **security personnel management**
    - **development personnel identification**
    - **personnel reliability**
      - **establishment of trust in people**
      - **security awareness**
    - **management of personnel outside the project (visitors, cleaning, maintenance, etc.)**
    - **IT resource management and maintenance**
    - **physical security resource management and maintenance**
- ✓ **conformity of the protection resources observed with the procedures**
- ✓ **verification of the procedure application evidence elements**
- ✓ **examination of the elements which prove that the procedures are applied**
- ✓ **interview with personnel to verify that they are familiar with the security policy, procedures and their own responsibility**

j. Elements to be verified for ALC_DVS.2:

- ✓ verification that protection resources exist for the TOE design information and samples
  - physical protection
    - area security
      - alarms
      - security administration
      - security personnel
    - access control
      - rights management (initialisation, verification, revocation, etc.)
      - access restricted to the project team
      - key, access code, badge, etc. management
    - secured physical storage
      - access code management (initialisation, renewal, etc.)
    - physical IT resource security
  - electronic protection
    - secured network
      - network partitioning
      - network administration
    - access control
      - authentication resources
      - rights management (assignment, revocation, verification, etc.)
      - password management (renewal, complexity, etc.)
    - backups
    - storage resources
  - organisational protection
    - information transfer management
    - security personnel management
    - development personnel identification
    - personnel reliability
      - establishment of trust in people
      - security awareness
    - management of personnel outside the project (visitors, cleaning, maintenance, etc.)
    - IT resource management and maintenance
    - physical security resource management and maintenance
- ✓ conformity of the protection resources observed with the procedures
- ✓ verification of the procedure application evidence elements
- ✓ examination of the elements which prove that the procedures are applied
- ✓ interview with personnel to verify that they are familiar with the security policy, procedures and their own responsibility
- ✓ **verification of the consistency of the different security measures and their suitability for the level of information to be protected**

APPENDIX B Visit programme

a. Visit programme introduction:

- Project name
- Evaluation tasks concerned
- Visit date
- Name and geographical address of the site concerned and, if necessary, designation of the rooms concerned
- Name of the evaluator carrying out the visit

b. Visit agenda:

- Visit start-up meeting with the visit team (evaluator and certifier) and the people met
  - Presentation of the visit team
  - Presentation of the visit objectives (specially for personnel who are not directly aware of the evaluation's requirements)
  - Presentation of the people met
  - Presentation of the site
- For each element to be verified (according to the procedures evaluated)
  - Visit format (verification on workstation, interview, etc.)
  - Personnel required for interviews
- Visit team debriefing
- Visit closure meeting with the visit team and the people met
  - Conclusion of the visit
  - Handover of any remark or non-conformity files

APPENDIX C Remark/non-conformity file

a. File identification

- File type (Remark / Non-conformity)
- File reference
- Project name
- Evaluation task concerned
- Visit date
- Name of the site concerned
- Evaluator's name

b. Description of the anomaly

- Detailed description of the anomaly

c. Developer's agreement

- Developer's agreement or disagreement
- Argument in the event of disagreement
- Date
- Developer's name

d. Corrective action proposal

- Description of the corrective action proposed
- Implementation deadline
- Date
- Developer's name

e. Corrective action validation

- Validation of the proposal by the evaluator
- Verification method planned
- Date
- Evaluator's name

f. File closure

- Reference of the corrective action evidence elements (document reference, visit, etc.)
- Evaluator's verdict
- Date
- Evaluator's name

APPENDIX D Visit report

a. Visit report introduction:

- Project name
- Evaluation tasks concerned
- Visit date
- Name and geographical address of the site concerned
- Evaluator's name
- Visit programme reference
- Visit methodology reference

b. Conduct of the visit

- For each element to be verified
  - Description of the verified elements
  - Identification of the roles of the personnel met
  - Evaluator's verdict
  - Reference of any files issued

c. Conclusion of the visit

- Summary of the inspected elements
- Evaluator's verdict

d. Remark and non-conformity files issued