Netherlands Scheme for Certification in the Area of IT Security (NSCIB)

Nederlands Schema voor Certificatie op het gebied van IT-Beveiliging (NSCIB)

NSCIB Scheme Instruction 07

Site Audits

Approved.....

Technical Manager NSCIB

Instruction	07
Report title	Site Audits
Date of issue	1 August 2017
Version	4.0
Distribution	Public
Filename	NSI_07_Site_Audits_v4.0.docx

TÜVRheinland®
Precisely Right.

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

1 Introduction

The purpose of the life-cycle support activity is to determine the adequacy of the processes and security procedures (measures) that the developer uses during the development (which includes everything up until production) and maintenance of the TOE. These procedures include the life-cycle model used by the developer, the configuration management, the security measures used throughout TOE development, the tools used by the developer throughout the life-cycle of the TOE, the handling of security flaws, and the delivery activity. The Common Criteria not only require to assess these procedures but also to gain confidence that these procedures are actually applied. To do this requires the following steps:

1. Review the documentation provided by the developer to understand the processes and procedures and to develop a plan of what is to be verified and how to verify that these processes and procedures are applied.
2. Gain confidence of the application of the processes and procedures. Confidence may be obtained through site audit(s) or through other evidence (e.g. completed review documents, logs of access control mechanisms).

According to the NSCIB documentation rules the need for a site audit must be determined during the preparation phase of the certification process. NSCIB certifiers endeavour to attend about 20% of all site audits based on a certification risk assessment and resourcing. This interpretation provides the rules for determining the necessity of performing a site audit and the procedure an ITSEF has to follow for performing site audits.

2 Waiver site audits

The CC and the CEM recommend the evaluator to perform site audits in order to gain confidence of the application of the described processes and procedures. This gives the possibility to use other means of acquiring evidence of compliance. At the kick-off meeting it can be decided to waiver auditing of a developer site by the ITSEF if the developer and evaluator request so. A waiver will be based on the following considerations:

- The general intention is to limit site audits as far as possible with NO site audits done by default for evaluations at EAL3 or below. This however does not imply that gaining confidence that processes and procedures are applied is not to be performed. In case insufficient or confusing evidence is available, the evaluator and/or NSCIB certifier may judge a site audit is needed after all.
- Re-use of the results of a previous site audit is possible only if that audit has taken place no more than 2 years before the issuance of the ETR of the current evaluation.
- Re-use of the results of a previous site audit is possible only in case that audit involved the same (version of) ALC requirements and methodology as applicable to the current evaluation. Any deviations of the ALC requirements and methodology must be assessed and mitigated or shown to not impact the re-usability.
- Re-use of the results of a previous site audit is possible only in case that audit was for a similar product using the same development and production processes and procedures (and in case of a production site also: the same equipment). A statement written by the developer addressing this is considered sufficient input for the assessment whether the site audit results can be re-used. In case the developer statement identifies (minor) changes a proper argument of why the changes have no impact is acceptable.
- Re-use of the results of a previous site audit taken place under another SOG-IS qualified scheme is possible if the required information as detailed in a Site Re-use Report (SRR) is available. This SRR information (see chapter 7) must be validated by the scheme under which it was issued. This can be done by listing it in the Certificate Report of the encompassing evaluation[1], or any other declaration from the other scheme to NSCIB.

[1] Like this is done with an ETR for Composition

- If there is a Site Certificate issued based on the applicable guidelines[2] a Site Security Target and a Certification Report are publicly available. The AST requirements (determining the minimum content of an SST) do not cover all the information as required for a SRR (the same for CR). Therefore some information might be missing. This missing information still needs to be provided. See chapter 7.1 for an identification of the not covered information. The preferred way of addressing this is to create an SRR as part of site certification.
- Re-use of the results of a previous site audit taken place under another CCRA qualified scheme is possible if both the full audit report and the required information as detailed in chapter 7 is provided.

3 The process of re-using site audit results

The evaluator shall, as part of the reporting for the ALC activities, justify that the site can be re-used by re-using its evaluation. This involves showing:

- The re-used audit satisfies the waiver considerations described in chapter 2 above.
- The re-used site is used in the re-using evaluation in a manner consistent with the audit. This based upon the following considerations:
  - The site activities relevant for the re-using evaluation were in the scope of the re-used audit.
  - For each of these site activities the associated interactions are 'compatible' with the sites with which the site 'interfaces' in input and output type and shipment method[3].
  - Any site re-use comments are addressed appropriately.

4 Generating Site Re-use Reports

A developer of a site to be audited under NSCIB can ask the ITSEF and the CB to facilitate re-use for future projects. To facilitate this re-use:

- The ITSEF creates a SRR (see chapter 7).
- The CB, after approval of the SRR, will list the SRR in the Certification Report (CR) and so declare suitability for re-use following this process.

Notes:

- This is the same process as used for the ETR for Composition document (created in case of e.g. Smart Card evaluations).
- In case of a Site Certification, creation of an SRR and listing it in the CR will be done by default (as the standard SST and CR do not contain all information necessary for re-use).

5 Site audits

5.1 Preparation

The CB will allow the execution of an site audit based upon the following considerations:

- The site audit checklist has been submitted to the NSCIB certifier at least 2 weeks before the date the audit is planned.
- The ALC reporting material has been provided and approved.

[2] At the date of this interpretation these are defined in: http://www.commoncriteriaportal.org/files/supdocs/CCDB-2007-11-001-SiteCertificationProcessv1-0.pdf

[3] This is very similar to how a certified platform is handled in a composition. For the definition of 'interaction' please refer to chapter 7 second bullet item.

Note that the same site audit checklist is also distributed to the developer in order to allow them enough time to read the questions, prepare the answers and prepare to facilitate the audit.

Depending on the TOE, the size of the site, the maturity of the developer, and the amount of information to be checked, the following guidelines are given:

- The ITSEF shall in principle assign 2 auditors to perform the site audit. The lead auditor shall be the person that has drafted the ALC material and checklist and acts as the spokesperson towards the developer. He shall also be responsible for drafting the site audit report and finalising the ALC material. The second auditor will normally take notes and acts as a backup for the lead auditor.
- If the site audit will be performed as part of a Smart Card evaluation, the schedule should allow for 1-2 days per site. An increased site audit time shall also be considered for those evaluations where communication problems because of language differences are likely to exist.

In case there is not that much information to process during a site audit (e.g. small site, re-visit) the ITSEF can deviate from the above guidelines, but this has to be agreed upon during the preparation phase of the certification process.

Considering that audits are typically strictly time-bounded, sampling of the site audit checklist may be necessary. The ITSEF is encouraged to discuss the sampling strategy with the certifier prior to the audit. This sampling strategy chosen must not be disclosed to the developer prior to the audit execution. Intent is to reduce the risk that the sample chosen by the ITSEF is unacceptable to NSCIB, while keeping the developer's preparation complete.

5.2 Checklist

The checklist must at a minimum, cover the following elements (when applicable) together with an explanation of how they are related to the CEM and the ST:

Physical security

- Site (Plant and building) security
- Transportation between buildings
- Personnel access granting / revocation

Logical security

- Network security
- Workstation and server security
- Personnel authorisation granting / revocation

Configuration management

- Shipping in / out
- Tracking items between development/production plants
- TOE version management (also across sites)

The checklist must also include an overview showing how the sites together realise the TOE. The overview must include all interactions (shipment) with the customer.

5.3 Execution

In order to have an efficient site audit it is strongly preferred that the site Security Manager, with knowledge of the physical and logical security measures, is available during (parts of) the site audit. Also the availability of a site Quality Manager with knowledge of the location of (written) procedures is preferable as their presence can help speed up the site audit.

6 Specific requirements for high-assurance evaluations

For evaluations where a VAN.5 requirement is present, the applicable JIL guidelines for site security[4] must be followed. Specific care shall be taken regarding access and distribution of all material and information related to the development and production of the TOE. This should be secured in such a way that the confidentiality and integrity (including protection against unauthorised disclosure, unauthorised modification or replacement and theft) is ensured.

Note that for some TOEs it is possible that the confidentiality of the design is not important and that in these cases only the integrity shall be secured. Examples of such TOEs are Open Source products or other secure products that cannot be successfully attacked using design or implementation information.

7 Content requirements for audit re-use

This chapter first provides some starting points and then defines the minimum set of information necessary for re-use of audit results under the NSCIB. In this chapter the individual information items are listed. With the intention to make this information available in a uniform layout a template for a Site Re-use Report (SRR) is also provided (in annex A).

The starting points for defining the minimum set of information required for re-use is:

- A site is a physical location where certain activities are performed. These activities are often called services[5]. The activities consist of process steps (e.g. development, testing, production step A). Some services do not involve process steps (e.g. a data centre providing the service: access to servers).
- To use such activities, interaction with the site is needed. The interaction is the fixed logical or physical shipment method, its description includes the type of input or output being shipped. For some services the input/output type is not relevant. Example: A data centre providing a 'data storage' service. The shipment method is the secured network across which the information is transferred. The input/output type is not relevant, any type of file could be read or written.
- The site to be re-used has been approved. This implies it is not needed to include details on why things are secure, that requirements are met etc.
- Re-using the activities of a site is possible only if:
  - the set of re-used activities is (a subset of) the activities covered by the re-used audit.
  - the interactions associated with the re-used activities are the same as the interactions covered by the re-used site audit.
- The information must be such that it is possible to determine:
  - that the site is being re-used in a way that was covered by the re-used audit.
  - that the situation at the site is still the same.

7.1 Minimum set of information

This section defines the minimum set of information needed for audit results re-use.

As explained in chapter 2, a Site Certification SST and CR do not include all the information needed for audit re-use. The list below shows what is and what is not included through the use of superscripted $^{+}$ and $^{-}$ symbols.

- Identification of ITSEF having performed the audit $^{+}$

[4] At the date of writing this is: http://sogis.eu/documents/cc/domains/sc/JIL-Minimum-Site-security-Requirements-V1.1(for_trial_use).pdf

[5] For the remainder of this chapter either one or both of the terms ‘activities’ and ‘services’ are used as considered appropriate. They however mean the same.

- Ø Unique ID (e.g. name and city) of the audited site [+]
- Ø High level type of site activity (e.g. development, testing, mask shop, data center) [+]
- Ø Name and address of the site [+]
- Ø Audit date [- 6]
- Ø Evaluation Scheme under which the audit was performed [+]
- Ø Certification ID as part of which the audit was performed [+]
- Ø ALC requirements met by the site and at which AVA_VAN level (e.g. ALC_CMC.4, ALC_CMS.5, ALC_DVS.2, ALC_LCD.1 and ALC_TAT.2 at AVA_VAN.5 level) [- 7]
- Ø Other security requirements that were covered as part of the audit (e.g. JIL MSSR) [-]
- Ø Maintained security of the configuration items: [-]
    - o Integrity: yes / partial (details must be listed under re-use notes),
    - o Confidentiality: yes/no
- Ø Document ID/title and version [+]
- Ø Edition history showing author, ITSEF approver's name and reason for update [-]
- Ø For each of the site activities a description detailing:
    - o Name of the activity (e.g. development, mask production) [+]
    - o Short (1-4 sentences) description of the activity (unless obvious from the activity name) [+]
    - o The development, production and configuration management tools used for the activity including their versions [-]
    - o All interactions including: [-]
        - § For logical shipment across a secure network: the network name
        - § For other shipments a reference (document name & section number) to the specific section(s) describing the shipment method.
    - o The area(s) involved in the activity. Make sure area names are such that in case a developer would move an activity to another area this would be detected. E.g. do not use 'Server room', use actual room numbers instead. [-]
- Ø Re-use remarks: Anything that is relevant for re-use of the site and its activities. [-]

  Some re-use remark examples:
    - o Sometimes at a site certain (most likely: production) steps do not maintain integrity properly. Though this means the site fails certain requirements this did not fail the evaluation in which it was involved. The integrity not properly maintained issue was mitigated by some other step performed at another site. Describe the issue and:
        - § In the SRR of the site where the issue was caused describe the required step to mitigate it. Include the ID of the site that mitigates the issue
        - § In the SRR of the site where the issue was mitigated describe the mitigating step such that it also becomes clear which issue was mitigated. Include the ID of the site where the issue was caused.

[6] Not included in CR by some schemes (e.g. ANSSI)

[7] This is not correctly covered by the site security AST requirements.

- Sometimes activities depend upon activities provided by other sites. List them here. Some examples:
  - A development site that depends upon an external data centre that provides access to the configuration management servers.
  - A data centre that physically manages its servers but for logical management depends upon another site performing IT management.

Some other more concrete examples:

- The site provides production step XYZ as a service. The site does not destruct scrap, it returns ALL scrap to its user. The shipment method used for scrap is the same as for functional products. In re-use situations it must be assured the user/customer of the site securely handles returned scrap.
- The site assembles PCBs. As part of the production steps the integrity of these PCBs is verified through optical, X-Ray and electrical inspection. Any failing PCBs will be rejected. In re-use situations, security requirements on the PCB manufacturer are not needed.

7.2 Site Re-use Report (SRR) template

See annex A.

Annex A

<ITSEF logo>

Site Re-use Report
<Site ID>

<type of site activity, e.g. mask shop>

Site	<Site name> <Full site address>
Audit date	<YYMMDD>
Document ID/title	<title or ID of this Site Re-use Report>
Document version	<version of this Site Re-use Report or 'See edition history'>
Document author	<name of author or 'See edition history'>
Evaluation Lab	<name>
Evaluation Scheme	<name>
Underlying Certification ID	<ID>
Security requirements	<e.g. ALC_CMC.4, ALC_CMS.5, ALC_DVS.2, ALC_LCD.1 and ALC_TAT.2 at AVA_VAN.5 level> <Document reference> <Document reference> …
Maintained security	Integrity: <yes/partially (details listed under re-use notes)> Confidentiality: <no/yes/partially (details listed under re-use notes)>

Edition history

Version	Date	Description	Author	ITSEF approver
0.1	<YYMMDD>			

Site description

Site activities:

- Activity #1:
  - <Name of the activity>
  - <Short activity description of the activity (unless obvious from the activity name)>
  - The development/production/test/configuration management tools used:
    - <Tool#1 including version>
    - <Tool#2…>
    - <…>
  - Interactions:
    - <Interaction #1 using method ABC>
    - <Interaction #2 using method DEF>
    - <…>
  - Area(s) involved:
    - <Area #1>
    - <Area #2>
    - <…>
- Activity #2:
  - <…>
- <…>

Re-use remarks:

- <Re-use remark #1>
- <Re-use remark #2>
- <…>