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 June 2018
Version	4.1
Distribution	Public
Filename	NSI_07_Site_Audits_v4.1.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 instruction 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 if the required information as detailed in a Site Technical Audit Report (STAR)[1] is available. This STAR must be validated by the scheme under which it was issued. This can be done by listing it in the (Site) Certification Report of the encompassing evaluation[2], or any other declaration from the other scheme to NSCIB. The developer shall provide a written statement whether the site audit results can be re-used, i.e. the situation at the site is still the same. In case the developer statement identifies (minor) changes, a proper argumention of why those changes have no impact is acceptable.

  Note that a STAR can be made available as a result of a normal product certification or alternatively as a result of a site certification process based on the applicable guidelines[3].
- Re-use of the results of a previous site audit is possible only if the STAR has been issued no more than 2 years before the planned issuance of the ETR of the current evaluation.

[1] See: http://sogis.eu/documents/cc/domains/sc/JIL-Site_Technical_Audit_Report-template-V1-0.pdf

[2] Like this is done with an ETR-for-Composition

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

3 Re-using previous site audit results

This chapter first provides some starting points and then provides guidance on the evaluation activities necessary for re-use of audit results under the NSCIB.

A site is a physical location where certain activities are performed. These activities are often called services. 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 evaluator shall, as part of the reporting for the ALC activities, justify that the site can be re-used by re-using its evaluation results. This involves demonstrating:

- The re-used audit satisfies the waiver considerations described in chapter 2 above.
- The results of re-used site audit are based on 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.
- The re-used site is used in the re-using evaluation in a manner consistent with the re-used site audit. This based upon the following considerations:
    - The re-used site audit is for a similar product using the same development and production processes and procedures (and in case of a production site also: the same equipment), i.e. site is being re-used in a way that was covered by the re-used audit.
    - The site activities relevant for the re-using evaluation were in the scope of the re-used audit, i.e. the set of re-used activities is (a subset of) the activities covered by 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.
    - Any site re-use comments are addressed appropriately.

Note that the site to be re-used has been approved. This implies that it is not needed to include details on why things are secure, that site requirements are met etc.

4 Site audits

4.1 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.

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 due to 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.

4.2 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.

4.3 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.

4.4 Validity of ALC results

As the date of approving the STAR, ETR or issuance of the certificate may have consequences for the re-usability of the relevant ALC activities, there must be a limit defined for the validity of ALC results. Internationally it is agreed that this validity is limited to 6 months. This means that the maximum time frame between a site visit and the approval of the STAR or ETR can be no longer than 6 months. If this time frame is exceeded, the evaluator will need to provide argumentation to the certifier why the results can still be re-used. The certifier reserves the right to request a renewal/verification of the related activities.

5 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.

6 Generating Site Technical Audit 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. The relevant box in the application form must be checked to make this request. To facilitate this re-use:

- The ITSEF creates a STAR (see [5]).
- The CB, after approval of the STAR, will list the STAR in the Certification Report (CR) and so declares suitability for re-use.

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 a STAR and listing it in the CR will be done by default.

[4] At the date of writing this is: http://sogis.eu/documents/cc/domains/sc/JIL-Minimum-Site-Security-Requirements-V2.1(for_trial_use).pdf

[5] See: http://sogis.eu/documents/cc/domains/sc/JIL-Site_Technical_Audit_Report-template-V1-0.pdf