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 12

Project Communication

Approved.....

Technical Manager NSCIB

Instruction	12
Report title	Project Communication
Date of issue	10 August 2020
Version	1.5
Distribution	Public
Filename	NSI_12_Project_Communication_v1.5.docx

TÜVRheinland®
Precisely Right.

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

1 Purpose of this document

To make sure that certification project related communication between all involved parties is done in a way that ensures that all relevant information will be exchanged in an appropriate manner.

2 Communication point-of-contacts

This NSCIB Scheme Instruction (NSI) is written to standardise the project related communication between the sponsor, the IT Security Evaluation Facility (ITSEF) and the certifiers of the Certification Body (CB).

The point-of-contacts for each certification project will be defined in the application form submitted by the sponsor and ITSEF to TÜV Rheinland Nederland. From the sponsor side these contacts are usually the project/product manager and the certification manager. From the ITSEF side these are usually the evaluation project manager and the lead evaluator.

The NSCIB works with certifiers from TrustCB who are appointed per certification project. The name and email address of the appointed certifier will be communicated by TÜV Rheinland Nederland to the sponsor and ITSEF after acceptance of the application form. The work performed by the certifier is monitored by a governmental certification monitor whose name is also communicated after acceptance of the application form.

3 Communication arrangements

3.1 Electronic communication

All certification related information exchange by electronic means (typically emails) that is addressed to the CB shall include the certifier and the general email address of the governmental certification monitors (nscib@nlncsa.nl). For certification tasks requiring a single point of monitoring, the commercial certifier is responsible for providing the certification monitor with all final evaluator deliverables at the conclusion of the certification activities ready for approval by NLNCSA.

The only exception is information related to financial aspects as this is only exchanged with TÜV Rheinland Nederland.

Project related email communication to the CB shall be identified by the certification/project ID as assigned by the CB (see NSI_06_Certification_ID_numbering) in round brackets in the subject line.

Please note that emails, including attachments, should not exceed a total size of 16MB due to mail server limitations.

3.2 Paper communication

All hard copies sent by the sponsor, the ITSEF or TÜV Rheinland Nederland shall be sent by regular mail or courier. Sending hard copies is strongly discouraged, but will be used to send the original signed certificate from TÜV Rheinland Nederland to the sponsor.

3.3 Confidential exchange of information

The commercial encryption program PGP (or open source equivalent GPG) shall be used to assure the confidentiality and integrity of information of a sensitive or proprietary nature that is exchanged by electronic means. This shall be done as an encrypted document or zip-file stored on a ITSEF operated (s)ftp server, cloud service, or as an attachment to an unencrypted email body. No s/mime or encrypted mail bodies shall be used. Please note that emails, including attachments, should not exceed a total size of 16MB due to mail server limitations.

Before sensitive or proprietary information is exchanged, PGP public keys (2.048/4.096 bit RSA/DSA) are exchanged between the identified point-of-contacts. The public keys of the TrustCB certifiers and the general NSCIB public key can be found on the NSCIB website. TÜV Rheinland Nederland should not receive any sensitive or proprietary information via email and will not be able to decrypt such information.

3.4 Types of information exchange

Evaluator deliverables like the Evaluation Technical Report and all other documents specified in the Evaluation Work Plan shall be submitted by the ITSEF to the certifier, and optionally to the sponsor.

Also all information exchange between sponsor and ITSEF of evaluation related technical matters shall be copied to the certifier using the rules as stated in sections 3.1 and 3.3 above. Examples of such information exchanges are:

- Minutes of meeting;
- Technical discussions;
- Evaluation process related issues;
- Preliminary reports/presentations.

Additionally, the certifier shall receive monthly status updates as required by section 5 of this instruction.

At the end of a project the certifier delivers a draft Certification Report to both the sponsor and ITSEF for technical review before the Certification Report is finalised and a certificate is issued and published.

3.5 Document format and language

All project communication and documents shall be in (UK) English or Dutch.

Documents shall be delivered in pdf format that allows to copy text from the document and to add notes. If available, a MS-Word / MS-Excel / MS-PowerPoint version of the pdf document can be requested for practical purposes.

All documents shall be labelled with an unambiguous document number, a version number, a date, and the certification ID as assigned by the CB. All sensitive or proprietary information shall be labelled as such. It is not required to use this labelling on every page.

A version numbering method shall be used that uniquely identifies a document. Any changes in a document shall result in a new version number and a new date. When a new version of a document is delivered, a clear method for marking changes between two formally delivered versions shall be applied to ease determination of these changes.

4 Minutes of Meetings and actions

During a project several meetings are being held and in accordance with the scheme procedures it is expected that the ITSEF records the outcome of these meetings by taking minutes and actions. No full meeting minutes are required to record every aspect of discussion, but rather these minutes serve as a record of any actions, verdicts and conclusions made during the meeting. This section provides the requirements for the content of the Minutes of Meetings (MoM) and on the actions noted in them. The goal of these requirements is to have a harmonised way in which the certifier is able to perform oversight by tracking and tracing actions and to conclude that all relevant information is included in his project dossier.

4.1 Requirements on MoMs

For all Minutes of Meetings, the following requirements apply:

- The date, time, location and attendees of the meeting shall be recorded;
- All documents and presentations that the lab has delivered for discussion at the meeting shall be listed by name and version;
- All revised documents and presentations coming out of the meeting shall be listed by name and version. Ideally, outputs of a meeting, should be attachments to the MoM;
- Intermediate conclusions and decisions made in regard to a specific document or presentation shall be recorded;
- A reference shall be made to the list of action items arising from the meeting (e.g. the version of Monthly Status Report, MSR (see section 5.2) in which the action items are recorded);

- The final conclusion of the meeting shall be recorded (see also NSP#6 for the 4 possible outcomes). This also includes a verdict on each of the documents and presentations discussed at the meeting.

4.2 Requirements for notation of action items

For the notation of action items (AIs), the following requirements apply:

- One identifier per action item in order to trace the action via the monthly reports;
- When the action relates to a document or presentation, the action item should refer to that document or presentation, including its version and location within the document or presentation (e.g. section number, slide number);
- The action should be self-explanatory, not relying on (undocumented) discussion in the meeting for clarity;
- Also, when an action is closed, the action item should clearly state how the actions was closed, e.g. by reference to the document or presentation where the action was closed;
- Per action item it shall be noted whether the certifier has approved its closure.

4.3 Requirements for tracking of action items

The set of action items (AIs) generated as a result of a meeting shall be transferred to the Monthly Status Report (MSR), as the single place where AIs are tracked. The ITSEF will update the status of the AIs to indicate how the item has been addressed. The certifier is ultimately responsible for the decision as to whether an AI may be closed.

As described in NSP#06, the status of AIs is reviewed as a standard agenda item at the start of the next meeting.

5 Evaluation Work Plan and monthly project status updates

According to the NSCIB documentation rules an Evaluation Work Plan must be agreed upon during the preparation phase of the certification process. This Evaluation Work Plan shall contain the elements described in Annex B of the NST_01_NSCIB_Application_Form template and forms the baseline for the evaluation and certification work.

As projects usually continue for several months it is expected that the agreed Evaluation Work Plan becomes outdated due to changes in scope, staffing, priorities and/or scheduling. This section provides the rules an ITSEF has to follow for informing the CB on relevant changes to the Evaluation Work Plan and requires a monthly project status update.

5.1 Changes related to the Evaluation Work Plan

An Evaluation Work Plan forms the baseline for the evaluation and certification work. As it is agreed upon by all involved parties it cannot be changed or executed in a different way by a single party. Possible changes that might have an impact can be categorised as follows:

- *Re-scheduling of milestones; these include both deliverables and review meetings;*
  The assigned certifier(s) expects to review documents and attend review meetings based on the agreed planning. They reserve time in their agenda which is difficult to re-allocate if deliverables are not submitted at the agreed date. The same is also true for any re-scheduling of meetings.
- *TOE scope changes;*
  The TOE scope is reviewed during the preparation phase, and if necessary discussed at a project kick-off meeting, and is accepted as being a valid TOE scope by the Certification Body. This is formally agreed in the review of the ASE report. Changes to the TOE scope mostly have an impact on the evaluation work already performed and could in extreme cases even result in inappropriate removal of security features or inappropriate additions of assumptions. In any case these changes must be reported as soon as possible so that their impact against the certification agreement can be determined. This may potentially lead to additional certification costs.

- *Evaluation scope/approach changes;*
  Changes to the evaluation scope (e.g. more or less development sites to be audited), additional/different deliverables or when additional review meetings are needed always have an impact on the certifiers oversight activities and could lead to additional certification costs.
- *TOE name/identifier changes;*
  Changes to the TOE naming or its identifier must officially be reported by the sponsor to TÜV Rheinland NL in copy to the assigned certifier(s). Such changes are relevant for the Certificate and its related Certification Report, and also to any in-evaluation entry on the scheme website, which must be updated to reflect the new name/identifier. As these changes might also have an impact on existing deliverables, the ITSEF must also be aware.
- *Project staffing/ITSEF personnel assignment changes.*
  The certifier(s) only accept deliverables that are authored by the evaluators listed in the Work Plan. NSCIB rules require the ITSEF to only assign qualified CC evaluators who are known to the Certification Body and have successfully passed the NSCIB CC examination.

An update to the Evaluation Work Plan is mandatory when there is a change to the evaluation scope/approach that requires a **contractual change** to reflect additional certification activities.

It is not ***always*** the case that all evaluation scope/approach changes require an update to the EWP, but this is the most likely indicator that the EWP needs to be re-issued. For example, a decision to discuss the ALC site audit checklist in EM1 rather than EM2 is a change of evaluation approach, although this decision can be agreed with the certifier and recorded in a monthly status report without an update to the EWP. While a decision to separate the Lifecycle (ALC) site audit checklist into a meeting of its own would require a contractual change to cover the certifier effort for an additional meeting, and that should be reflected in an updated EWP. Another borderline case is if a face-to-face evaluation meeting is switched to being a remote/virtual meeting. This would not require a contractual change to the certification activities (as no additional cost is incurred) but it does mean a change of evaluation approach, from an in-person meeting to remote meeting, and needs to be recorded. In this instance, it is sufficient to record this in the Monthly Status Report.

Typically the majority of other changes can be handled through Monthly Status Report. In particular, the EWP does **not** need to be updated for re-scheduling of milestones, TOE name/identifier changes and project staffing/ITSEF personnel assignment changes. In addition, most TOE scope changes can also be recorded solely through the Monthly Status Report, without the need for an update of the EWP.

If a change to TOE scope also means an evaluation scope/approach change, then that is likely to require an update of the EWP.

5.2 Monthly project status updates

The ITSEF Project manager who is responsible for the evaluation work is required to provide a Monthly Status Report of the project. This status update is a document with a unique title and date and shall contain sections as follows:

- *Section one:* provides administrative project details, including the time period on which the project status updates reports on and the latest approved Evaluation Work Plan;
- *Section two:* provides reference to the status of outstanding action items derived from the MoM of previous evaluation meetings. The requirements on the notation of actions in section 4.2 also apply here;
- *Section three:* describes proposed changes structured along the categories defined above in section 5.1. Changes that need to be permanently captured should be incorporated in a newer version of the Evaluation Work Plan once the assigned certifier(s) have approved a Monthly Status Report.
  - Re-scheduling of milestones: Changes to previously reported milestone dates should be indicated (identifying whether the changed date is a proposed date or one that has already been agreed with the commercial certifier). For meeting dates, the plan should indicate whether the commercial certifier should confirm travel plans (this may result in additional certification charges if the certifier incurs cancellation/re-booking fees). The ITSEF should indicate any factors that cast doubt about the confidence of reaching a milestone date.

- TOE scope changes: Any changes to the TOE scope defined in the Application Form (and associated ST) must be reported by the ITSEF.
- Evaluation scope/approach changes: Any changes to the evaluation activities being performed by the ITSEF must be reported, For example, repeat of developer tests has to be moved from ITSEF facilities to the developer site.
- TOE name/identifier changes: If there is a change to the TOE name/identifier (or the organisation name with who has entered into a contract with TÜV Rheinland for certification) the certification agreement and website entry should be reviewed, and the update reported to TÜV Rheinland as necessary.
- Project staffing/ITSEF personnel assignment changes: Personnel leaving and personnel joining the evaluation team must be reported.

The Monthly Status Report shall be submitted to the assigned certifier(s) ***on the first working day of every month*** as long as the monitoring phase continues. The certifier shall endeavour to provide written feedback within 3 working days.