SOG-IS Recognition Agreement
Management Committee
Policies and Procedures

Document ID: SOG-IS-shadow-VPA–v2.0
Subject: Conducting shadow Certifications and VPAs

Purpose

1 The purpose of shadow certification is to determine that a Certification Body applying for acceptance as a Compliant Certification Body under the SOG-IS Mutual Recognition Agreement (SOG-IS-MRA) complies with the requirements in Annexes B, C, D and G of the SOG-IS-MRA.

2 The SOG-IS-MRA also calls for periodic assessment of Evaluation and Certification Schemes (refer hereinafter as "the Scheme", or "Qualifying Scheme", or "the applicant Scheme", as applicable) operated by compliant Certification Bodies. The purpose of a Voluntary Periodic Assessment (VPA) is to determine that the constitution and procedures of the Certification Body under assessment continue to comply with the requirements of the SOG-IS-MRA.

3 The focus of the shadow certification/VPA program is to ensure that the oversight activities of the Certification Body being assessed meet the SOG-IS-MRA including the necessary technical skills and evaluation techniques, and that its ITSEFs[1] have the appropriate equipment and competencies and - for recognition at higher levels - that its ITSEFs meet the requirements in applicable JIL documents[2]. The principles of certification that are used by the Certification Body in overseeing its evaluation facilities should be applied during the shadow certification/VPA. There are three phases involved in performing the shadow certification/VPA: preparation, site visit, and reporting.

4 The process is as comprehensive and objective as possible, using checklists (see Annex A, B and C) to assist the shadow certification/VPA team. However, since the assessment team is based upon experts, and may wish to make assessments based upon a common understanding of the team of state of the art and operating

[1] All ITSEF(s) currently approved by the scheme for that domain.
[2] E.g. For Technical Domain "Smart cards and Similar Devices", refer in particular to document "Minimum ITSEF requirements for security evaluation of smartcards and similar devices".

practices[3] the team need not restrict themselves to these lists and can report additional findings. The JIWG will discuss, during their review, whether these views are shared by all, and, where appropriate, will incorporate a new item into the lists for use by future shadow certification/VPAs.

Scope and applicability

5 This procedure covers three types of shadowing/VPA that may be required by the SOG-IS Management Committee:

a) Type 1: When a Certification Body (CB) applies for recognition against any of the Common Criteria Evaluation Assurance Levels 1 through 4 or ITSEC Assurance Level E1 through E3

b) Type 2: When a Compliant CB applies for recognition at a higher level in a specific technical domain

c) Type 3: When a Compliant CB applies for recognition at a higher level in a new technical domain for which there are no existing compliant CBs

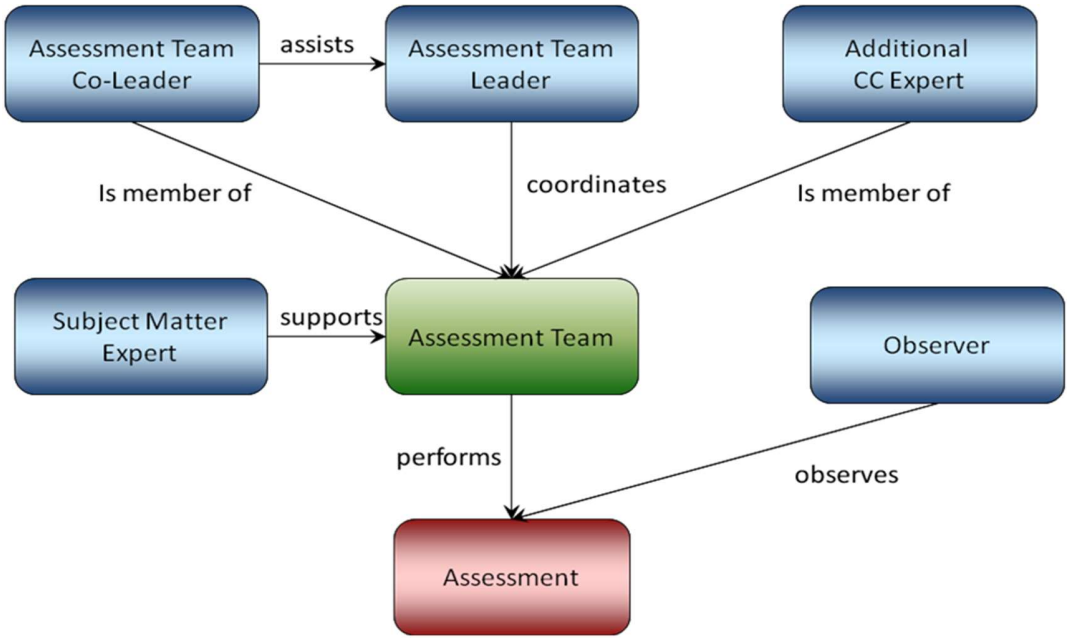
6 Any differences between Types 1 and Type 2 above are identified within this procedure, while the process to be used for Type 3 is contained in Annex B to this procedure.

7 The remaining part of this procedure is related to the application of Common Criteria. It is assumed that a Scheme which is capable of performing the Common Criteria Evaluation and Certification activities is also capable of performing the equivalent level of ITSEC activities.

Overview

8 In accordance with the SOG-IS-MRA Annex G.3 the primary assessment team consists of 2 CC experts (Leader and co-Leader) selected from 2 or more Qualified Participants. This primary assessment team can be extended with additional CC experts from other or the same Qualified Participants.

3 As discussed and agreed by JIWG and/or relevant subgroups



9 For a Type 2 assessment the primary assessment team shall be selected from Qualified Participants in the requested technical domain.

10 Each CC expert in the assessment team shall have a minimum of the following skills/experience:

a) two years as a certifier at a SOG-IS Compliant CB in the relevant technical domain, if applicable; and

b) knowledge of the ITSEF licensing process within the Scheme operated by Compliant CB .

11 For a higher level assessment (Type 2 above defined) the assessment team can be assisted by subject matter experts in the technical domain(s) concerned. Those experts may be certifiers themselves, but that is not essential.

12 It is also highly recommended that the assessment team members have participated in previous shadowing or VPAs either as observers or team members. Ideally these should be assessments performed under SOG-IS, but CCRA assessment experience is also of benefit.

13 The assessment can be observed by observers proposed by other Participants, subject to agreement by the MC.

14 The applicant may present to the MC any concern they have about the choice of the assessment team members and observers, for example in case of a conflict of interest.

15 The assessment activities will be carried out in three phases. The preparation phase will involve review of the Scheme documentation by the members of the assessment team in order to become familiar with the Scheme's policies and procedures. The site visit phase will consist of a two-weeks visit by the assessment team to the Scheme in order to assess the Scheme's technical competence in performing evaluations. The exact duration of site visit will depend on the possible reuse of CCRA VPA, and, for Type 2 assessment, on the number of ITSEF(s) and on the number of Technical Domains the scheme is qualified or applies for. The assessment will conclude with the reporting phase.

16 The assessment team will document their findings in an assessment report that will be delivered to the JIWG. The JIWG will review and agree/modify the report reflecting its common view and then provide the report to the MC for voting. Following this vote the MC Chair will notify the Scheme of the final decision.

Scheduling Assessment Activities

17 In order to schedule the assessment activities, the Scheme applying for acceptance as a Qualified Participant into the SOG-IS-MRA (Type 1) or for acceptance as a Qualified Participant at a higher level in a specific technical domain (Type 2), must send a written application to the Management Committee in accordance with Annex G of SOG-IS-MRA.

18 In case of need of confirmation that the Scheme continues to comply with SOG-IS-MRA requirements, JIWG will inform the Qualified Participant and will task an assessment team to perform the VPA.

19 In addition to Annex G.3 the applicant has to submit the required number of candidate products (see table 1), for which the applicant Scheme has followed the evaluation project, for review by the assessment team. In general the candidate products shall cover all technical aspects of the audit.

20 For acceptance as a Qualified Participant at a higher level in a specific technical domain (Type 2 above defined) the applicant must

a) submit at least one product per technical domain per considered qualified ITSEF, for which the applicant Scheme has followed the evaluation project, for review by the assessment team, and

b) supply details of every ITSEF that it considers to be qualified to evaluate[4] at the higher level in that technical domain.

[4] Including those it anticipates approving within the next 12 months

21 Requirements for minimal number of products subject to evaluation under the shadow certification/VPA are summarized in Table 1.

Evaluated products	Type 1	Type 2
Minimal No. of candidate products	2	min. 1 per requested Technical Domain, and per each ITSEF applying*
No. of product subject to evaluation under the shadow certification	1	min. 1 per requested Technical Domain, and per each ITSEF applying*
* EXAMPLE		
number of Technical Domains requested		2
number of ITSEFs applying for a higher level of evaluation on the 2 Technical Domains		2
minimal number of products evaluated under the shadow certification		2 x 2 = 4

Table 1 Minimal number of products subject to evaluation under the shadow certification/VPA

SHADOW CERTIFICATION

22 In case of a **new applicant (Type 1 and Type 2),** the Management Committee chairman will acknowledge receipt of the application within three weeks and will forward the application to the JIWG for consideration. The JIWG will review the application, define the scope of the assessment, set up an assessment team and tasks the assessment team (i.e. assessors , observers and subject matter experts) for the shadow certification within two months since the JIWG notification by the MC. After its review the JIWG will notify the applicant of its decision.

23 The assessment team will then send the applicant a request for candidate products. The applicant will respond to the request providing to the assessment team a list of candidate products (and ITSEFs) within one month. After its review the assessment team will notify the JIWG and the applicant about the selected product. The JIWG has the right to veto within 1 month after notification. The assessment team will arrange the date of the audit with the applicant.

24 The following time diagram summarizes the scheduling activities in case of a new applicant (type 1 or type 2).

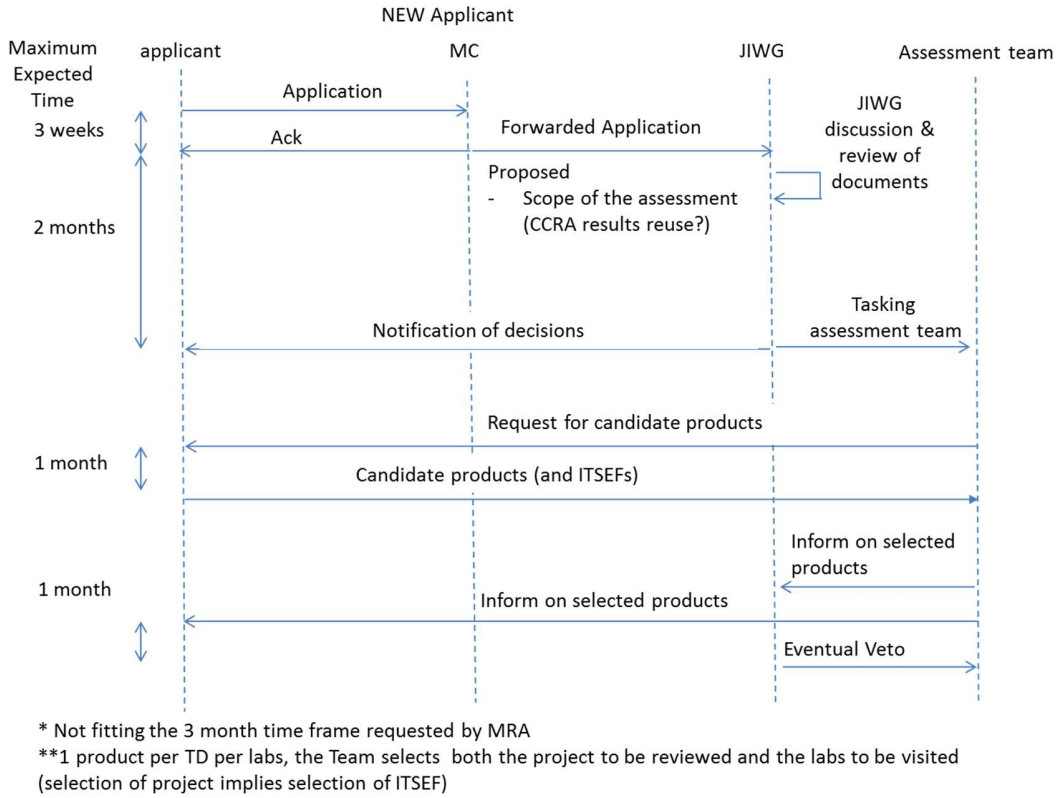


Fig. 1 - Time Diagram for new applicant assessment activities

VPA

25 In case of a **VPA,** the JIWG chairman will inform the Qualified Participant and the JIWG will task an assessment team for the VPA to be carried on.

26 The JIWG will report to the Management Committee on a regular basis including a proposed date for the assessment activities, the list of auditors (i.e. assessment team, observers and subject matter experts) and proposed dates for the ITSEF(s) site visit(s).

27 The assessment team will then send the Qualified Participant a request for candidate products. The Qualified Participant will respond to the request providing to the assessment team a list of candidate products (and ITSEF) within one month. After its review the assessment team will notify the JIWG and the applicant about the selected products (and ITSEFs). The JIWG has the right to veto within 1 month after notification. The assessment team will arrange the date of the audit with the applicant.

28 The following time diagram summarizes the scheduling activities in case of a VPA.

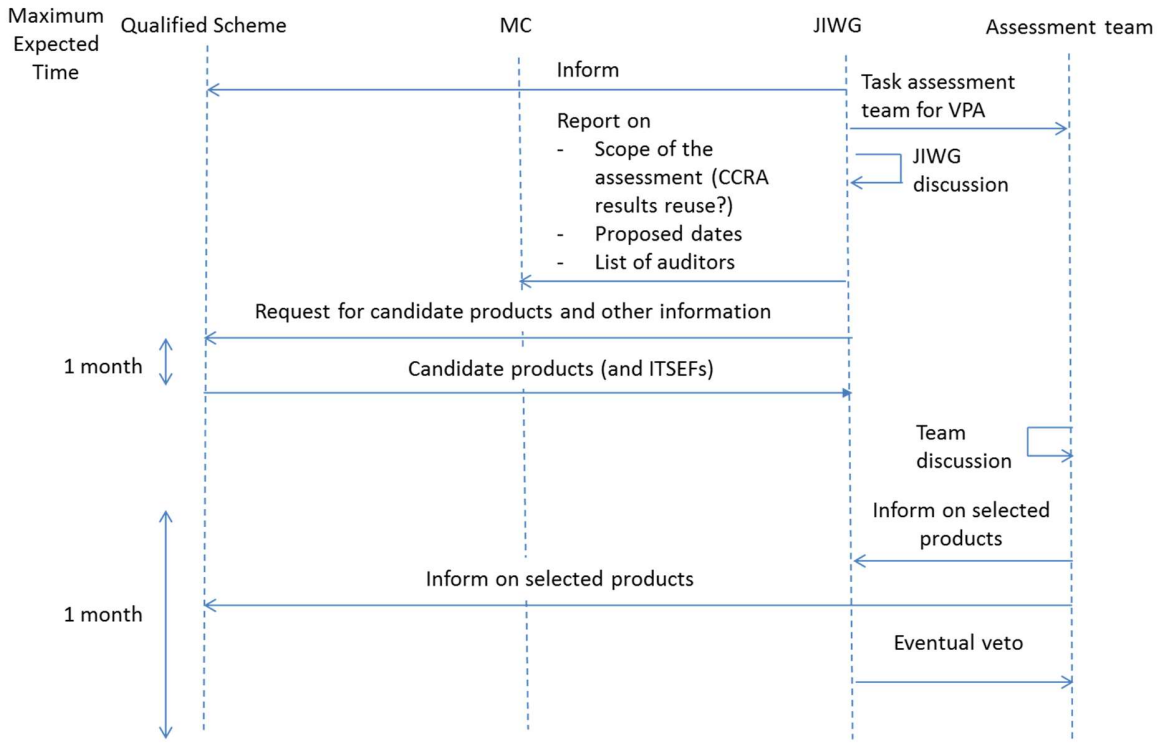


Fig. 2 - Time Diagram for VPA assessment activities

Responsibilities of Scheme Being Assessed

29 All written documentation and communications for the assessment activities must be provided in English at least 4 weeks before the audit date, to include:

a) A full description of the scope, organization, and operation of the applicant's Evaluation and Certification Scheme including:

- The title, address, and principal point of contact of the CB;
- The CB Quality Manual;
- The subordination of the CB and the statutory or other basis of its authority;
- The system for overseeing the general management of the Scheme, for deciding questions of policy, and for settling disagreements;
- The procedures for certification;

- The titles and addresses of the Evaluation Facilities participating in the Scheme, their status (commercial or governmental) and their licensing scope;
- The licensing/approval policy and the procedures for licensing Evaluation Facilities;
- The rules applying within the Scheme for the protection of commercial and other sensitive information;
- A description of the information by which the CB ensures that Evaluation Facilities:
  - Perform evaluations impartially;
  - Apply the mutually agreed IT criteria and methods correctly and consistently; and
  - Protect the commercial and/or sensitive information involved.

b) The latest issue of the Scheme's Certified/ products list;

c) Two or more SOGIS-MRA candidate certificates and Certification Reports issued under the oversight of the applicant.

d) A statement about the effects of all national laws, subsidiary legislation, administrative regulations, and official obligations applying in the country of the applicant and directly affecting the conduct of evaluations and certifications/validations or the recognition of SOG-IS-MRA certificates; and

e) A statement that the applicant is not bound by or about to be bound by any law, subsidiary legislation, or official administrative order which would give it or the IT products or Protection Profiles to which it awards SOG-IS-MRA certificates an unfair advantage under the SOG- IS MRA or which would otherwise frustrate the operation or intention of the SOG-IS-MRA.

30 Where the CB has already been granted a Qualifying status through a similar procedure within the framework of another international MRA, all necessary information on this Qualifying status and on that MRA. For acceptance as a Qualified Participant at a higher level in a specific technical domain (Type 2) the Qualified Scheme must provide a list of all the ITSEFs that they consider to be qualified for that domain[5] and a description of the evidence used when licensing these evaluation facilities;

31 During the site visit, English will be spoken, unless the Scheme and the assessment team unanimously agree upon another language.

[5] Including those that it anticipates approving within the next 12 months

32 One part of the assessment activities during the site visit will involve a review of at least one evaluation that has been completed or is close to being completed within the Scheme. (In the case of an application for a higher level in a specific technical domain (Types 2 above defined) the evaluation must be for a product within that domain and involve appropriate attack methods/vulnerability search at the highest level).

33 Although the evaluations for chosen products submitted for consideration need not be entirely complete, there must be records showing that significant evaluation analysis and certification activities have been performed, and that the majority of the evaluation report (including at least one vulnerability analysis round) has been delivered to and analyzed by the certification team.

34 For shadowing, in addition to the selected products, the Scheme may also provide the assessment team with information on (up to) another two evaluations which were completed in the 12 months prior to the start of the assessment activities. If the assessment team has sufficient time and resources, they will review these evaluations during their site visit and, if they are found to be compliant with SOG-IS-MRA requirements, will recommend to the MC that permission be given for the Scheme to officially certify these evaluations to receive mutual recognition.

35 The Scheme is responsible for preparing, documenting and providing general information on the candidate products. This information will be provided to the assessment team for their review and selection. The information provided by the Scheme to the assessment team should include:

a) a brief overview of the product,

b) the status of the evaluation (if not completed, then indicate what parts of the evaluation have been completed and what remains to be done),

c) the target EAL (and augmentation, if any), and

d) any Protection Profile compliance claims.

36 The assessment team will select at least one candidate evaluation(s) to be assessed by the assessment team during the site visit and the ITSEF(s) to be visited and will notify the Scheme and the JIWG within one month since the receipt of the information on the candidate products being under evaluations.

37 The Scheme will identify a Point of Contact who will be the individual responsible for facilitating the assessment activities and for interacting with the assessment team leader and the JIWG.

38 The Scheme Point of Contact is responsible for:

a) Coordinating the site visit(s) dates and location(s) with the assessment team,

b) Delivering the Scheme materials to the assessment team during the Preparation Phase at least 4 weeks before the audit date,

c) Coordinating any required ITSEF(s) visits with the assessment team (For acceptance as a Qualified Participant at a higher level in a specific technical domain (Type 2 above defined) the JIWG will decide the selection of ITSEF(s) to be visited),

d) Arranging all necessary approvals to allow the assessment team to perform the CB and ITSEF(s) site visits and to have access to all information required to complete the assessment activities,

e) Coordinating the assessment agenda for the Scheme, including scheduling certifiers for assessment team interviews and briefings, ensuring the availability of materials to be reviewed during the site visit, etc.,

f) Providing the assessment team with the ability to have copies and printouts made for use during the site visit;

g) Providing secure storage, if required, for the assessment team's documents (e.g. lunchtime, overnight);

h) Being generally available to answer questions and resolve issues that may arise during the site visit,

i) Coordinating the review of the assessment report by Scheme representatives, and

j) Providing feedback to the assessment team leader on the assessment draft report.

39 The Scheme must have a private room(s) available that is (are) large enough to accommodate the assessment team and Scheme personnel during the site visit(s). Such room will serve as the meeting room throughout the site visit. Accessibility to records and Scheme personnel will be needed throughout the site visit in the meeting room.

Responsibilities of Assessment team Leader

40 One member of the assessment team will be designated the team leader. The assessment team leader is responsible for the following tasks:

a) Coordinating the receipt of materials from the Scheme,

b) Coordinating the decision regarding the selection of the candidate products (and ITSEFs) and notification to the assessed scheme and the JIWG

c) Drafting the site visit agenda (and for acceptance as a certificate producer at a higher level in a specific technical domain (Type 2 above) the selected ITSEF(s) to visit), and coordinating it with the Scheme,

d) Coordinating and completing the assessment draft-report at the end of the site visit,

e) Delivering the assessment final report to the JIWG, and if necessary,

f) Monitoring the Scheme's resolution of outstanding issues resulting from the assessment process.

Preparation Phase

41 The assessment team should begin preparation approximately four weeks before the site visit. The Scheme shall provide the assessment team with access to all written policies and operating procedure documents as stated in para 29 four weeks before the site visit. Electronic and/or hardcopy documentation have to be provided, depending on the preference of the assessment team members and nature of documentation needed. The assessment team should focus their review of the documentation on gaining an understanding of the Scheme's standard operating procedures.

42 The assessment team leader will coordinate the review of materials during the preparation phase. If there is a large amount of material to be reviewed, the team may divide it so that members review different portions of the documentation. The team leader will also draft and finalize the site visit(s) agenda, with input from the team members, at the conclusion of the preparation phase. The site visit(s) agenda must be forwarded to the Scheme no later than one week before the site visit(s). It is recommended that the assessment team leader should maintain close contact with the Scheme Point of Contact during the preparation phase to keep the Scheme informed of areas that will require further investigation during the site visit.

43 In the case CCRA Shadow/VPA report is available it can be considered as input to the relevant Shadow/VPA process.

Site Visit Phase

I. Determine that the constitution and procedures of the Scheme being shadowed comply with the requirements of Annexes B, C, D and G of the SOG-IS Agreement on the Recognition of SOG-IS certificates (SOG-IS-MRA).

44 The checklist in Annex A of this document shall be used to determine that the constitution and procedures of the Scheme under assessment comply with the requirements of Annexes B, C, D and G of the Arrangement on the Recognition of SOG-IS certificates (SOG-IS-MRA).

45 This checklist is to be used to determine if the processes that the Scheme uses to provide its certification services are sufficient to ensure effective oversight of evaluations and to ensure that successful certifications comply with the Common Criteria and the Common Evaluation Methodology. The checklist is applicable to any Scheme under assessment, although if the Scheme has been accredited in its respective country by a recognised Accreditation Body (in accordance with ISO/IEC 17065, EN 45011 or ISO/IEC Guide 65), then the results of that accreditation may be used in the review of the Scheme's adherence to the requirements of SOG-IS-MRA Annex C. The reason for reuse is that the SOG-IS-MRA Annex C requirements correspond exactly to the EN 45011 requirements in the 1989 standard. (This standard has been superseded by the 1998 standard, which has added additional requirements.)

46 If checking the procedures of the Scheme is necessary, this can be accomplished by checking the information required in G.2a of the SOG-IS-MRA according to G.3 of the SOG-IS-MRA. This check must be completed before the assessment process commences. Nevertheless, the assessment team should check that the Scheme is applying its procedures. This can be done at the site visit (see below) for the particular certifications being assessed.

II. Perform the assessment.

47 For Type 2 shadow certifications/VPAs, the assessment team should allocate two full weeks for the site visit. If the assessment is completed in a shorter period of time, the team need not stay the full two weeks.

48 The assessment team shall have access to all evaluation and certification documentation that was used by the Scheme during its oversight process; and shall be permitted to observe all activities carried out during the Scheme's oversight

process. If an evaluation team/certifier meeting occurs during the site visit, the assessment team should observe the meeting.

49 The assessment team should not independently completely review the work of the evaluation facility, which will be covered by EN-ISO/IEC 17025 or EN 45001. However, the assessment team should assess whether the deliverables available to the Scheme are of sufficient quality to allow the Scheme to determine that the Scheme evaluation was conducted in accordance with the appropriate methodology.

50 For Type 2 shadow certification/VPA, the assessment team will make a determination of ITSEF technical competence by

a) visit of technical lab in the ITSEF site,

b) interviews with evaluators on technical items related to the Technical Domain and its specific attack methods.

51 Findings corresponds either to

a) non-conformities that are linked to a requirement from the list available in annex A or to common understanding of state of the art and operative practices that are not met (or not fulfilled). The latter will be discussed with the JIWG and could, where appropriate, be incorporated as a new item into the lists for use by future shadow certification/VPAs.

b) or observations that correspond to improvement proposals made by the assessment team, not directly linked to annex A requirements.

A non-conformity could be either critical or non-critical. A critical non- conformity challenges the reliability of the results established by the audited scheme. The assessment team shall analyze and describe the impact of each critical non - conformity.

52 At the end of the site visit, the assessment team should present the list of findings (at least the draft list of non-conformities associated to their criticality level). The assessment team should provide the final list of non-conformities (associated to their criticality level) not later than 4 weeks after the site visit to the assessed scheme.

53 If non-conformities have been identified the Scheme shall provide to the assessment team, within one month after receiving the final list of non-conformities (associated to their criticality level), an action plan associated to a timescale to implement those actions.

54 If it is not possible to gain agreement on the identified non-conformities with the Scheme, the Scheme shall explain its disagreement, highlight it in the documented list of findings, and provide it to the assessment team within one month after receiving the final list of non-conformities (associated to their criticality level).

55 Once disagreements have been resolved, the Scheme shall provide to the JIWG, within one month after solving the disagreements, an action plan associated to a timescale to implement those actions.

Reporting

56 To finalize their work, the assessment team will produce a report that summarizes and explains their findings (see Annex G.4 of the SOG-IS-MRA).

57 The report should be agreed internally within the assessment team before its submission to the JIWG. If the assessment team cannot agree internally, then majority and minority opinions shall be included in the report.

58 Scheme disagreement on findings can be incorporated to the report; in any case Scheme disagreements have to be provided no later than one month after the report.

59 The report shall also present the position of the assessment team on the relevance of proposed action plan to cover the findings. If evidence that cover critical non conformity is provided before issuance of the VPA report, the Team can reconsider the criticality of the non-conformity and shall document this change in the report.

60 SOGIS assessment team should also check CCRA Shadow/VPA report. In case CCRA recommendations relevant to SOGIS Shadow/VPA have been correctly addressed, the resolution adopted has to be included in the report. If such recommendations have not been correctly addressed, the CCRA recommendations should be included in the report also as a SOGIS recommendations.

61 However, recommendations from the SOGIS assessment team included in the report shall be clearly separated from these set up by the CCRA assessment team. Additionally, an unique and unambiguous identifier will be provided by the assessment team for each recommendation to distinguish between previous SOGIS-VPA recommendations and new ones.

62 The report will be produced within three months after the site visit and will be reviewed by the Scheme prior to distribution to the JIWG.

63 The report shall provide one of four possible verdicts:

• Pass	The Scheme has met all requirements and no further action is required.

• Pass with controlled (minor) non-conformities	The Scheme has not met all requirements, but has provided a relevant actions plan and an acceptable timescale for correcting the non-conformities identified by the assessment team. There is no remaining critical non-conformity identified in the report. If the planned timescale is respected and all the corrective actions have been applied there is no need to inform MC: checks on the actions will be performed at the next VPA. If for some reasons the planned timescale has not been respected, the assessed scheme is expected to produce a rationale and send it to the MC.
• Action required before pass	For a shadow certification the Scheme must implement the fixes to the non-conformities identified by the assessment team before the Scheme is accepted as a Qualifying Participant (or compliant CB in a specific technical domain). For VPA the Scheme must implement the fixes to the non-conformities within a delay set by the MC. The Scheme will then be reassessed (only on the scope of the non-conformities). The Scheme should refrain from issuing certificates during this 'warning' period.
• Reject	The Scheme has not met the requirements and hasn't provided relevant updates of its process in the period defined by the MC. It should not be accepted as/continue as a Qualifying Participant (e.g. non conformity regarding the SOG-IS–MRA and the current procedure has been identified).

64 The assessment team leader (or a suitable representative with full knowledge of the assessment) is then expected to attend the next JIWG meeting to discuss the assessment. The JIWG will review all remarks and reach a consensus on their

applicability to all schemes and the rationale for why they should be observed by all. Where relevant, appropriate additions will be made to the assessment checklist to assist future assessment teams.

65 *Disagreements reporting:* In the case of disagreement on findings, the report should include both the Scheme position and the Team position on the issue, in order to require arbitration.

66 *Arbitration on disagreements:* the JIWG is in charge of arbitrating disagreements. The assessment team leader then updates the report to reflect the JIWG position and provides the updated report to the Scheme.

67 *Final review and transmission to MC:* The JIWG reviews the final report for consistency and forwards it to the MC.

68 *Final decision:* The MC Chair initiates a MC review of the final report. The final approval is performed by vote. The MC Chair will convey the final decision to the Scheme in writing within a target of two months following receipt of the final report from the JIWG.

69 In case of shadow certification of all types, if the Scheme is accepted, the MC Chair shall update the list of SOG-IS-MRA Qualified Participants accordingly. In case of VPA, no changes are necessary.

70 If action before pass is required, the applicant Scheme will be provided with 30 days to propose a resolution to all recommendations and 90 days to implement them. Progress will be monitored by the assessment team leader and reported to the JIWG Chair until all actions have been completed. If difficulties arise, the assessment team leader will facilitate negotiations between the JIWG Chair (in consultation with the MC) and the Scheme being assessed. The MC Chair (in consultation with the MC) will be the final arbiter. Upon satisfactory completion of all required actions, the assessment team leader shall notify the JIWG Chair and the MC Chair. The MC Chair shall then notify the Scheme and update the list of SOG-IS-MRA Compliant Certification Bodies accordingly.

71 *Warning' period:* When the conclusion of a VPA is *Action required before pass*) the MC will set the timeframe for a second visit, in order to check that the non conformities have been addressed (or suitable processes are in place if no suitable evaluations have occurred within the timeframe to provide evidence; in this case the MC may plan the next VPA earlier than the usual 5 years period. The VPA team in charge of this second visit is ideally the same team as the original one.

72 *Support on non-conformities remediation during the 'warning' period:* The Scheme may ask the JIWG to review their approach to addressing non-conformities. JIWG advices are non-binding and the second VPA visit team will be able to justify different conclusions.

73 If the Scheme is rejected, the MC's response shall provide a summary of the reasons for rejection and the evidence on which the decision is based. In case of shadow certifications no changes to the list of SOG-IS-MRA Qualified Participants are necessary. In case of VPAs the list is changed accordingly.

Annex A

Checklist for Determining that the constitution and procedures of the Certification Body under assessment comply with the requirements of Annexes B and C of the Arrangement on the Recognition of SOG-IS certificates (SOG-IS-MRA).

74 **Key:** "Y" is "yes", "N" is "no" and "I" is "inconclusive"

Item	**Verdict (Y/N/I)**	**Evidence**	**Rationale/Notes**
Check that the services of the Certification Body are to be available without undue financial or other conditions.			
Check that the procedures under which the Certification Body operates are to be administered in a non-discriminatory manner.			Requirement of (C.1)
Confirm that the Certification Body is to be impartial by checking that it has permanent staff responsible to a senior executive enabling day-to-day operations to be carried out free from undue influence or control by anyone having a commercial or financial interest in the certification.			Requirement of (C.2)

Check that the Certification Body has and makes available: a) a chart showing clearly the responsibility and reporting structure of the organisation; b) a description of the means by which the organisation obtains financial support; c) documentation describing its Evaluation and Certification Scheme; d) documentation clearly identifying its legal status.			Requirement of (C.3)
Check that the personnel of the Certification Body are to be competent for the functions they undertake.			Requirement of (C.4) This evidence comes in part from the actual findings during the site visit phase, although formal qualifications and experience and ISO/IEC 17065, or EN45011 accreditation may also provide a part of the evidences. In case of recognition at higher levels in one or more specific Technical Domains the certifier technical skills analysis result has to be share by at least two subject matter experts (as this criteria is subjective).

Check that information on the relevant qualifications, training and experience of each member of staff is maintained by the Certification Body or by the organization's personnel department and kept up-to-date			Requirement of (C.4)
Check that, in case of recognition at higher levels in one or more specific Technical Domains, a representative of the Certification Body attend the specific Technical Domain Communities regular meetings.			Attending JIWG subgroups provides the most up to date view of work undertaken by those groups. CB representatives are expected to attend at least 50% of these meetings (as in JIWG TORs). The representative need not be a CB certifier (e.g. external expert) but need to be active in CB activities (e.g. Supporting CB in the specific Technical Domain certification activities or monitoring certification activities in that domain) and to convey the knowledge directly to all involved certifiers.
Check that personnel have clear, up-to-date, and documented instructions pertaining to their duties and responsibilities available to them.			Requirement of (C.4)

Check that, if work is contracted to an outside body, the Certification Body ensures that the personnel carrying out the contracted work meet the applicable requirements of Annex C of the SOG-IS-MRA.			Requirement of (C.4) [Great care needs to be taken if certification work is contracted to an outside body. A Certification Body contracting out certification work should provide a rationale of the appropriateness of contracting. Development of guidance is a task, which can be done by an outside body with the relevant experience and qualifications.]

Check that the Certification Body maintains a system for the control of all documentation relating to its Evaluation and Certification Scheme and that it ensures that: a) current issues of the appropriate documentation are available at all relevant locations; b) documents are not amended or superseded without proper authorisation; c) changes are promulgated in such way that those who need to know are promptly informed and are in a position to take prompt and effective action; d) superseded documents are removed from use throughout the organisation and its agencies; e) those with a direct interest in the Scheme are informed of changes.			Requirement of (C.5) [For item e), those with a direct interest in the Scheme will include all product vendors who use the Scheme, the evaluation facilities, and customers of certified products in government departments and companies in the critical national infrastructure. It may also include system integrators who produce systems for government.]

Check that the Certification Body maintains a record system to suit its particular circumstances and to comply with relevant regulations applied in the jurisdiction to which the Participant is subject.			Requirement of (C.6) [The record system used should contain sufficient information to enable an assessment to be performed. It should enable an observer to determine that the certification was performed in an impartial, objective way and adhered to the appropriate criteria and methodology.]
Check that the record system includes all records and other papers produced in connection with each certification; it is to be sufficiently complete to enable the course of each certification to be traced.			Requirement of (C.6)
Check that all records are securely stored for a period of at least five years.			Requirement of (C.6)
Check that the Certification Body has the required facilities and documented procedures to enable the IT product or Protection Profile certification to be carried out in accordance with the applicable IT security evaluation criteria and methods.			Requirement of (C.7)

Check that evaluation facilities fulfil the following two conditions: a) they are accredited by an Accreditation Body officially recognised in the country concerned; and b) they are licensed or otherwise approved by the Certification Body responsible for the management of the Scheme.			Requirement of (B.3) CB licensing process shall permit the scheme to estimate the ITSEF technical skills In case of recognition at higher levels in one or more specific Technical Domains the ITSEF technical skills has to be analysed by the Team. Analysis results have to be shared by at least two subject matter experts (as this analysis is subjective).
Check that the Evaluation Facility demonstrates, to the satisfaction of the Certification Body, that it is technically competent in the specific field of IT security evaluation and that it is in a position to comply in full with the rules of the Scheme concerned.			Requirement of (B.3) [Evidence for this check will not involve a separate check on the evaluation facility. All that is required is that the Certification Body describes how it determines that evaluation facilities are technically competent.] For acceptance as a certificate producer at a higher level in a specific technical domain (Type 2 above) the assessment team will visit each of the two selected Evaluation Facility and make a determination of its technical competence.
Check that the Certification Body confirms that the Evaluation Facility has the ability to apply the applicable evaluation criteria and evaluation methods correctly and consistently.			Requirement of (B.3) For acceptance as a certificate producer at a higher level in a specific technical domain (Type 2 above) the assessment team will visit each of the two selected Evaluation Facility and make a determination of its technical competence.

Check that CB has clear rules on how to decide when (and when not) to witness the site visit performed by the Evaluators during evaluation activities.			
Check that the Certification Body confirms that the Evaluation Facility meets stringent security requirements necessary for the protection of sensitive or protected information relating to IT products or Protection Profiles under evaluation and to the process of evaluation itself.			Requirement of (B.3)
Check that the Certification Body has drawn up, for each IT Security Evaluation Facility, a properly documented agreement covering all relevant procedures including arrangements for ensuring confidentiality of protected information and the evaluation and certification processes.			Requirement of (C.8) It is suggested that the CB includes in their licensing procedures the relevant requirements for evaluation work performed by an ITSEF on different locations, including locations outside the country.

The Certification Body is to have a Quality Manual and documentation setting out the procedures by which it complies with the requirements of Annex C of the SOG-IS-MRA. These are to include at least: a) a policy statement on the maintenance of quality; b) a brief description of the legal status of the Certification Body; c) the names, qualifications and duties of the senior executive and other certification personnel; d) details of training arrangements for certification personnel; e) an organisation chart showing lines of authority, responsibility and allocation of functions stemming from the senior executive; f) details of procedures for monitoring IT product or Protection Profile evaluations; g) details of procedures for preventing the abuse of Common Criteria certificates; h) the identities of any contractors and details of the documented			Requirement of (C.10)

Check that the Certification Body has adequate arrangements to ensure confidentiality of the information obtained in the course of its certification activities at all levels of its organisation.			
Check the application of the procedures to ensure the confidentiality of protected information			Requirement of (C.10)
Check that the Certification Body does not make an unauthorised disclosure of protected information obtained in the course of its certification activities under the SOG-IS-MRA.			Requirement of (C.10) [Check the Certification Body's procedures to ensure that they help prevent unauthorised disclosures. The assessment team should then ask to see all complaints against the Certification Body received by the Scheme. Checking for unauthorised disclosures is especially important if the information protection procedures of the Certification Body are not adequate.]
Check that the Certification Body produces and updates as necessary a Certified Products List available to the public. Each IT product or protection profile mentioned in the list is to be clearly identified. A description of the Evaluation and Certification Scheme is to be available in published form.			Requirement of (C.11)

Check that the Certification Body has procedures to deal with disagreements among itself, its associated evaluation facilities, and their clients.			Requirement of (C.12)
Check that the Certification Body undertakes periodic reviews of its operations to ensure that it continues to share the SOG-IS-MRA objectives.			Requirement of (C.13)
Check that the Certification Body takes appropriate administrative, procedural or legal steps to prevent or counter the misuse of certificates and to correct false, misleading or improper statements about certificates or about the Evaluation and Certification Scheme.			Requirement of (C.14) Check for a suitable process being in place
Check that the Certification Body is to have documented procedures for withdrawal of SOG-IS certificates and is to advertise the withdrawal in the next issue of its Certified Products List.			Requirement of (C.15)

Annex B

Process for Scheme (and ITSEF) Approval while creating a new technical domain (Type 3)

Introduction

75 The process defined here is available for the SOG-IS Management Committee to select when a group of SOG-IS schemes combine to create a new technical domain (as with the POI/Hardware boxes as the first example)

Approach

76 The schemes that have been involved in the development of the new domain, having produced the necessary domain definition, technical requirements, and protection profiles/supporting documents (possibly in conjunction with an associated technical community) will perform trial certifications (in cases where, for some schemes involved, this proves infeasible – for example where market conditions result in vendors involved in the trial selecting other schemes, then, at the discretion of the SOG-IS MC a suitable technical demonstration of competence may be substituted).

77 The trial should be based upon a full disclosure process for evaluations performed within the trial period where each of the certification bodies involved will have full access to all outputs from each evaluation. This is a much greater level of information than that which is involved in an assessment process and will lead to all schemes gaining a thorough understanding of all aspects of the evaluations. The certification bodies involved should analyse the disclosed information with a focus on vulnerability analysis and associated penetration tests and ensure that the evaluations have been consistently performed and take necessary actions to ensure that this is the case.

78 Evidence will be provided only during the meeting and will not be distributed to the auditors after the meeting.

79 The ITSEF will have to demonstrate its ability to perform the vulnerability analysis and the associated penetration tests.

80 Acceptance of Type 3 incoming requests will be limited to one year after the MC has approved the second CB under this process.

Annex C

Site visit phase, for Type 2 assessment

81 Site visit shall cover the whole technical domain(s) and shouldn't be only related to the reviewed candidate evaluation projects. In fact attack method related to technical domains has to be known and implemented by all scheme claiming a qualifying status.

CB site visit

Review of the project.

82 The assessment team with the support of subject matter experts shall examine all documentation that was used by the Scheme during its oversight process. Below is a list of documentation, including examination requirements, that is commonly available in most Schemes' oversight activities.

83 **Evaluators' work plans.** A work plan may be written by the evaluation facility prior to starting an evaluation, to describe the scope of the evaluation and how the evaluation team will perform its analysis. These should be examined in conjunction with the certifier's comments and the actual effort figures from the evaluation facility (if available) to determine that the certifier's oversight ensured that the scope of the evaluation was clearly defined, coherent and conformed with the Common Criteria requirements. The assessment team should take into consideration that "evaluator's work plan" is not defined in the CEM so content and scope of work plans may differ between Schemes.

84 **Security Targets.** These should be examined in conjunction with the Scheme's comments in order to gain an understanding of the security features and claims of the product, and in order to determine that the target of evaluation was clearly defined and coherent.

85 **Evidences on evaluation results.** These should be examined in conjunction with the certifier's comments on the technical reports to determine that they supply sufficient evidence to demonstrate that the Common Criteria assurance package claimed and reported in the certification report has been met in accordance with the Common Methodology. For acceptance as a certificate producer at higher level in a specific technical domain Evaluators' technical reports should be examined in conjunction with the certifier's comments on the technical reports to determine that they supply sufficient evidence to demonstrate that proper attack methods and other relevant guidance have been taken into account for vulnerability assessment.

86 **Evaluation observation reports.** These should be reviewed in conjunction with the evaluators' technical reports and the certifier's comments on the observation reports to determine that the Scheme ensured that the resolution to the observations was adequate.

87 **Certifier's review comments.** These should be reviewed in conjunction with the relevant evaluation team analysis to determine that they provide effective oversight of evaluation output and identify any assurance related deficiencies in that output.

88 **Minutes of evaluation team meetings.** These should be examined to determine that any technical issues have been resolved in a satisfactory manner.

89 **Scheme's internal technical records.** These should be reviewed in conjunction with the certifier's review comments to determine that all assurance related issues have been addressed adequately.

90 The documentation requested may be sent to the assessment team or it can be inspected at the Scheme's premises.

91 For an ongoing evaluation, not all of the documentation requested may be available. In this case, the assessment team should attempt to make up for any deficiencies in documentation during the site visit by requesting access to documentation on another product evaluation.

92 The documentation review will reveal areas for further questioning or comments, which should be discussed with the Scheme during the site visit. The assessment team may request further evidence for particular areas.

93 During the site visit, the assessment team, with the support of subject matter experts should cover areas commonly addressed in most Schemes' oversight activities. These areas include:

a) agreeing on responses to any questions or comments raised during the documentation review;

b) obtaining the current status of the evaluation being assessed (if the evaluation has not already been completed);

c) checking the application of the Scheme's procedures; and

d) reviewing how the Scheme resolves problematic or contentious issues relating to the certification of the assessed product evaluation.

94 The assessment team with the support of subject matter experts should check that all oversight activity is performed in accordance with Scheme procedures and that those procedures are adequate to oversee the evaluation.

CB procedures and competencies assessment.

95 In practice, it may not be possible to cover all required certification activities and a representative sampling of certifiers will take place by fully reviewing just one evaluation per technical domain during the CB visit. If necessary, the assessment team will require additional information from the other proposed evaluations in order to gain insight into the Scheme's full certification process.

96 Focus areas should include, but are not limited to the following:

a) CB personnel matters such as: skill level assessment, project assignments (based on what; how assigned), training (both of new personnel and ongoing skills training of more experienced personnel), conflict of interest/non disclosure agreement obligations, the types of personnel records maintained.

Remark: assigned CB ETR review team shall have the skills to challenge the evaluation work done by the lab. It doesn't mean that CB technical experts have to be involved every time but that the CB ETR review do understand the topics addresses in the ETR.

Full content of all ETR has to be reviewed to check that the lab fulfilled the evaluation activities as defined by the CC/CEM and related supporting documents. For VPA purpose, the CB shall show that it has reviewed the vulnerability analysis and penetration testing according to the state of the art as defined by the supporting documents and ad'hoc JIWG decisions.

b) CB records issues relating to: records maintenance – how long, what information is kept, how it is kept, who has access, how the records are used (i.e., personnel performance appraisals, technical decisions and precedents, etc.); how the technical decisions are recorded and promulgated.

c) Scheme evaluation facilities: how laboratories are licensed and how licensing is maintained; the role of certifiers in lab assessments, review of the finding detailed in the report of the biennial CB audits of the laboratories to cover the specific capabilities for the technical domains.

d) CB conflict of interest: what is the policy; how proprietary information is protected, and how conflict of interest and non-disclosure policies are implemented within the CB.

e) Technical consistency issues such as: how consistency is maintained between laboratories and across certifications; what type of Scheme oversight is implemented to ensure consistency and technical acumen of certifiers and ITSEF.

f) For technical domains the team will examine examples of CB action in that technical area assessing the certifier level of understanding of the state of

the art regarding attack methods in that domain, how the certifier knows when to bring in a technical expert and how the organisation supports this process. The team will also examine the involvement of internal technical experts (brought by the CB) in the approval process of some specific technical part of the certification and their interaction with the ITSEF experts. The involvement of the CB and internal technical expert in the oversight or witnessing of the ITSEF site visit task should be reviewed as well.

ITSEF site visit

97 For entry to the higher level of each technical domains the assessment team will also expect to examine the capabilities (equipment, knowledge and skills) of two associated ITSEF(s) from the list of all the ITSEF that the Scheme under assessment consider to be qualified for that domain.

98 Focus areas should include, but are not limited to the following:

a) ITSEF personnel matters such as: skill level assessment, project assignments (based on what; how assigned), training (both of new personnel and ongoing skills training of more experienced personnel), conflict of interest/non disclosure agreement obligations, the types of personnel records maintained.

b) ITSEF records issues relating to: records maintenance – how long, what information is kept, how it is kept, who has access, how the records are used (i.e., personnel performance appraisals, technical decisions and precedents, etc.); how the technical decisions are recorded and promulgated.

c) ITSEF conflict of interest: what is the policy; how proprietary information is protected, and how conflict of interest and non-disclosure policies are implemented within the Scheme.

d) Technical consistency issues such as: how consistency is maintained between evaluators; what type of ITSEF oversight is implemented to ensure consistency and technical acumen of evaluators.

e) For technical domains the team will examine if all necessary equipment are available, if all the qualification of personnel to use this equipment are available. The assessment team may also ask for demonstration of capability of the ITSEF regarding this equipment.