Common Criteria Recognition Arrangement
Management Committee

Operating Procedures

Document Number: 2005-06-21

Date: 31 May 2016

Subject: Conducting Voluntary Periodic Assessments of Schemes Participating in the CCRA.

Purpose

The Arrangement on the Recognition of CC certificates (CCRA) calls for periodic assessment of member Schemes. 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 CCRA.

Overview

VPAs of member Schemes will occur on a periodic basis (no more than once per five years). A team consisting of at least 2 qualified experts coordinated by the Executive Subcommittee and approved by the Management Committee, will perform the VPA.

VPA team members shall have a minimum of the following skills/experience:

- Two years as a Certifier at a Scheme, and
- Knowledge of the Evaluation Facility accreditation process within their own country.

It is highly recommended that the VPA team members have participated in previous shadowing or VPAs either as observers or team members. It is also recommended that team members should not be from the same nations for consecutive VPAs of the same Scheme.

The VPA will be carried out in three phases. The preparation phase will involve review of the Scheme documentation by the members of the VPA team in order to become familiar with the Scheme's policies and procedures. The site visit phase will consist of a one-week visit by the VPA team to the Scheme in order to assess the Scheme's technical competence in performing evaluation certifications. This part of the assessment will be done in the context of at least two certified IT products that are within the scope of the Arrangement that have been completed by the scheme as agreed upon by the Participants directly involved; these IT product evaluations shall be representative of what the

Scheme typically certifies. The VPA will conclude with a written report documenting the team's findings and recommendations.

During the reporting phase, the VPA team will document their findings and recommendations in a report that will be delivered to the ES. The ES Chair will then notify the Scheme of the findings.

The Scheme must address any issues raised during the VPA within six months of notification by the ES Chair. Once the ES has agreed that all findings have been addressed, the ES will provide the report to the MC and the MC Chair will notify the Scheme of the final decision.

Responsibilities of VPA Team Leader and Scheme Point of Contact

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

- Coordinating the delivery of materials by the Scheme,
- Organizing the site visit agenda and coordinating it with the CB,
- Coordinating and finalizing the VPA report at the end of the site visit, and
- Delivering the final VPA report to the Executive Subcommittee.

A representative from the Scheme will serve as the Point of Contact for the VPA. The Scheme Point of Contact is responsible for:

- Coordinating the date of the site visit with the VPA team,
- Coordinating all necessary Non-Disclosure Agreements with the VPA team prior to the site visit,
- Delivering the Scheme materials to the VPA team during the Preparation Phase,
- Coordinating the VPA agenda for the Scheme, including scheduling certifiers for VPA team interviews and briefings, ensuring the availability of materials to be reviewed during the site visit, etc.,
- Providing a private room for use by the VPA team during the Site Visit;
- Providing the VPA team with the ability to have copies and printouts made for use during the Site Visit;
- Being generally available to answer questions and resolve issues that may arise during the site visit,
- Coordinating the review of the VPA report by Scheme representatives, and
- Providing feedback to the VPA team leader on the report.

Issues

There are two primary issues that must be considered in the implementation of the VPA program:

1. Disclosure of vendor and/or laboratory proprietary information to the VPA team will only occur in the context of assessing the CB's technical competence. It is anticipated that the VPA team will review the ETRs and Observation Reports for the projects selected. However, review of evaluation evidence for the projects should not be necessary, except for the ST. This issue has a significant bearing on the conduct of the VPA and on the information that can be reviewed by the VPA team.

2. Unless it has been established under a law or statutory instrument, evaluation facilities need to be accredited by a recognised Accreditation Body. Verification of the validity of the accreditation, if needed, is the responsibility of the individual Schemes as a part of the licensing procedure. If a Scheme is following their procedures (assuming the procedures are designed to meet the CCRA), then it is acceptable for the VPA team to assume that the laboratories within a member Scheme are operating correctly and that the laboratories' evaluation results, once certified, are technically sound. Given this assumption, the VPA team should have no need to perform a direct review of evaluation team or laboratory records, except when included as part of a certification record.

Specific Guidance for VPA

Given the two primary issues listed above, the focus of the VPA Program should be to assess that the oversight activities of the member Schemes meet the CCRA. The principles of oversight that are used by the Schemes in working with their laboratories should be applied by the VPA team in performing the VPA of the Scheme. There are three phases involved in performing the VPA: Preparation, Site Visit, and Reporting.

All written documentation and communications for the VPA activities must be provided in English, to include:

1. A full description of the scope, organization, and operation of the applicant's Evaluation and Certification/Validation Scheme including:
    - The title, address, and principle 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/validation;
- The titles and addresses of the Evaluation Facilities participating in the Scheme and their status (commercial or governmental);
- The licensing/approval policy and the procedures for accrediting Evaluation Facilities;
- The rules applying within the Scheme for the protection of commercial secrets and other sensitive information;
- The procedures 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 confidentiality of sensitive information involved.

2. A copy of Annex A of this document, annotated with details in the "Evidence" column that summarize how the Scheme complies with each of the requirements in the checklist.
3. The latest issue of the Scheme's Certified/Validated products list;
4. Two or more Common Criteria certificates and Certification/Validation Reports issued under the oversight of the applicant;
5. 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 Common Criteria certificates; and
6. 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 Common Criteria certificates an unfair advantage under the CCRA or which would otherwise frustrate the operation or intention of the CCRA.

During the site visit, English will be spoken, unless the Scheme and the shadow team mutually agree upon another language. It is strongly recommended that all other evaluation evidence and evaluation outputs be provided in English.

Preparation Phase

Preparation should begin approximately four weeks prior to the site visit. The Scheme should provide the VPA team with access to all written policies and operating procedure documents. The Scheme should strive to provide this information in an unchangeable format (such as PDF). It is expected that all or much of this documentation will be available to the VPA team at least four weeks in advance of the site visit. However, if all policies and operating procedures cannot be delivered to the VPA team during the preparation phase, then time must be allocated during the site visit for this review. If the Scheme has previously undergone a VPA, a copy of the final report from the previous

VPA should also be provided. A copy of the final Shadow Certification Report should be provided for a Scheme's initial VPA. Electronic or hardcopy documentation can be provided, depending on the preference of the VPA team members. The VPA team should focus their review of the documentation to gain an understanding of the Scheme's standard operating procedures.

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

1. Scheme 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, what types of personnel records are maintained, performance reviews (who performs reviews, how often, and how reviews are applied to ensure the technical acumen of Scheme personnel).
2. Scheme 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 technical decisions are recorded and promulgated.
3. Scheme evaluation laboratories: how laboratories are accredited and how accreditation is maintained; what role certifiers have in lab assessments.
4. Scheme conflict of interest: review the policy, including how proprietary information is protected and how conflict of interest and non-disclosure policies are implemented within the Scheme.
5. 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.
6. Subsequent VPA activities should review policy changes or procedures implemented as a result of the recommendations from the previous VPA report.

The VPA team leader will coordinate with the CB to arrange for the review of materials by the VPA team 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 agenda, with input from the team members and the CB, at the conclusion of the preparation phase. The agenda must be forwarded to the Scheme not later than one week prior to the commencement of the site visit. It is recommended that the team leader maintain close contact with the Scheme Point of Contact during the preparation phase to keep the Scheme apprised of issues that will be further investigated during the site visit.

Site Visit

The site visit will allow the VPA team to gain confidence in the technical capabilities of the Scheme and to ensure that the written policies and procedures that were reviewed

during the preparation phase are being implemented by the Scheme. Time spent at the Scheme will allow the VPA team to further explore any issues that arose during the preparation phase.

The VPA team leader will coordinate the logistics for the site visit with the Scheme, but is expected to delegate responsibility for investigating issues and questions to other VPA team members throughout the visit. There may be parallel activities that occur during the site visit in order to accomplish more than one activity simultaneously.

The VPA team will perform the site visit approximately four weeks after receiving the Scheme's documentation. The site visit will consist of not more than five working days at the Scheme facility, with the final day allocated to drafting the VPA report and briefing the Scheme management on the recommendations and results.

Assessment of Technical Capabilities

The site visit will provide the VPA team with the opportunity to determine the technical capabilities of the Scheme's Certification Body (CB). The benefit of being on site at the Scheme is that the VPA team will be able to speak directly with members of the CB. Prior to interviewing CB representatives, the VPA team should review the material that is used to train certifiers. Material that is used to train certifiers may be formal or informal. Some items to be reviewed may include:

- coursework from training sessions;
- informal electronic discussions that deal with technical issues;
- mentoring program guidelines; and
- minutes or notes from certification body workshops.

After a review of training materials, members of the VPA team should interview individual certifiers in order to gauge their technical skills and knowledge of the CC and CEM. Technical issues discussed should focus on the application of the CC/CEM by a certifier for specific issues in the context of a certification procedure. Both junior and senior level certifiers should be interviewed, with different focus areas, depending on the certifier's experience level.

Issues that are suitable to discuss with a senior certifier include (but are not limited to) the following:

- the VPA team should present a technical issue and have the certifiers discuss the solution;
- ask the certifier to describe a recent technical issue that they've encountered on a certification and how the issue was resolved;
- ask the certifier to describe what he does to mentor junior certifiers;
- ask how the certifier promotes technical consistency (both among evaluation facilities and across certifications).

Issues that are suitable to discuss with a junior certifier include:

- ask the certifier to describe how they were trained;
- ask the certifier to describe a technical issue they've recently encountered on a certification and how it was resolved;
- ask the certifier to describe his plan for developing into a senior certifier, including milestones and timeframe.

At least four certifiers should be interviewed, depending on the size of the certification body. A pool of certifiers available to be interviewed should be selected by the CB. The VPA team should be provided with the names and information about each certifier's experience level, and then shall select the candidates to be interviewed. At the conclusion of the interviews, the VPA team members should discuss and document their findings as input into the final VPA report. Certifiers who were interviewed need not be mentioned by name; instead, general findings and impressions should be documented.

Implementation of Policies and Procedures

The second goal of the site visit is to ensure that the written policies and procedures that were reviewed during the preparation phase are being implemented by the Scheme. The VPA team should focus this part of the site visit on a review of Scheme records to demonstrate that the written policies and procedures are being followed. While the records reviewed may be considered Scheme protected information, vendor and laboratory records need not be reviewed, except when included as part of a Scheme record. The VPA team's purpose is to validate the implementation of the Scheme's policies and procedures. This focus will help to limit the amount of proprietary information that is accessed by the VPA team. If the team must review proprietary information, the Scheme may require non-disclosure agreements.

The VPA team should focus their review on the following areas:

- personnel records;
- certification records;
- conflict of interest policy; and
- technical consistency.

The activities associated with the review of the Scheme's policies and procedures may be more efficiently accomplished if the VPA team divides the areas outlined above, allowing each team member to focus on one or two.

Personnel Records

The VPA team must ensure that the Scheme (or the organization's personnel department) maintains information on the relevant qualifications, training, and experience of each member of the staff. The records maintained must be kept current. The team should be provided with information that describes all phases of the personnel process, including the hiring of a new certifier, his skills assessment, training, project assignment(s), and performance review. If possible, records that show this process for a single individual

should be reviewed, in order to confirm that the entire process is implemented as documented. If national privacy laws prevent review of an individual's personnel records, then that should be noted by the VPA team in the report.

Certification Records

The certification records for at least one completed certification should be reviewed, to ensure that they are being properly maintained. The records reviewed should include the initial submission for certification by an evaluation facility or vendor to the Scheme, certifier records generated (including notes, emails, etc.), any observation decisions and/or interpretations generated, and the resulting certification report and certificate. It is not necessary for all evaluation reports to be translated for the VPA, but the VPA team may require that the Evaluation Technical Report and Observation reports for the selected evaluations be translated. Although some of the certifier records may contain vendor and/or laboratory proprietary information, the records reviewed should be Scheme records only, and as such are controlled by the Scheme. This will help to mitigate the issue concerning the release of proprietary information to the VPA team.

Conflict of Interest Policy

Avoiding conflict of interest is an issue faced by all Schemes and as such, must be verified by the VPA team. Records associated with a potential/real conflict of interest should be reviewed, including identification of the initial issue, resolution, and follow up.

Technical Consistency

Technical consistency must be maintained across evaluation facilities and among certifiers. The VPA team should review records that demonstrate how consistency is maintained within the Scheme. The type of records to be reviewed may include:

- those that show dissemination of technical guidance to the certification body and evaluation facilities;
- records that show how a technical issue that impacted more than one certification was promulgated and applied to other certifications; and
- records demonstrating that technical issues were addressed in a consistent manner across the Scheme.

Compliance with CCRA Requirements

The checklist in Annex A of this document shall be used to determine that the constitution and procedures of the CB under assessment comply with the requirements of Annexes B and C of the CCRA.

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 either in accordance with ISO/IEC 17065 or its successors or in accordance with a national interpretation of ISO/IEC 17065 or its successors, then the results of the accreditation may be used in the review of the Scheme's adherence to the requirements of Annex C of the CCRA.

VPA Reporting

The VPA team will spend the final day of the site visit coordinating and finalizing the VPA report. The team should document their findings throughout the site visit in order to minimize the effort required to finalize the report at the end of the visit. The VPA report should document the findings of the team, including strengths and areas for improvement. Also included in the report will be a list of action items and a recommended timeframe for completion. The VPA team should meet with Scheme representatives to provide verbal feedback on the VPA and a copy of the draft report.

The VPA report shall provide one of three possible recommendations:

• Compliant	The Scheme complies with all CCRA requirements and no further action is required.
• Conditionally Compliant	The Scheme must implement recommendations made by the VPA team.
• Noncompliant	The Scheme has not met the requirements and should not continue as a certificate-producing nation.

The team leader is responsible for delivering the final VPA report to the Executive Subcommittee. The ES Chair will then notify the Scheme of the findings, and will add an item, for discussion of the VPA report, to the agenda for the next ES meeting.

Within six months of notification from the ES Chair, the Scheme must demonstrate that they have addressed any issues raised within the VPA report. The VPA team will update the VPA report to include details for how the recommendations were addressed by the Scheme, and will deliver the updated VPA report to the ES Chair. The ES Chair will provide the report to the MC Chair, who will initiate a 75-day commenting period within the CCRA nations. When unanimous consent is reached that the information provided in the report is internally consistent and that the conclusion follows from the evidence, the MC Chair will notify the Scheme of the acceptance of the findings in the report.

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 CC certificates (CCRA).

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

Item	**Verdict (Y/N/I)**	**Evidence**
Check that the services of the Certification Body are to be available without undue financial or other conditions. (C.1)		
Check that the procedures under which the Certification Body operates are to be administered in a non-discriminatory manner. (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. (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;		

Item	Verdict (Y/N/I)	Evidence
c) documentation describing its Evaluation and Certification Scheme; d) documentation clearly identifying its legal status. (C.3)		
Check that the personnel of the Certification Body are to be competent for the functions they undertake. (C.4)		[This evidence comes in part from the shadow certification check, although formal qualifications, experience, ISO/IEC 17065 (or its successors) accreditation may also provide evidence.]
Check that information on the relevant qualifications, training and experience of each member of staff is maintained by the Certification Body or by the organisation's personnel department and kept up-to-date (C.4)		
Check that personnel have clear, up-to-date, and documented instructions pertaining to their duties and responsibilities available to them. (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 CCRA. (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		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

Item	Verdict (Y/N/I)	Evidence
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. (C.5)		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. (C.6)		[The record system used should contain sufficient information to enable a shadow certification 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. (C.6)		
Check that all records are securely and accessibly stored for a period of at least five years. (C.6)		
Check that the Certification Body has the required facilities and		

Item	Verdict (Y/N/I)	Evidence
documented procedures to enable the IT product or Protection Profile Certification/Validation to be correctly carried out in accordance with the Common Criteria and related evaluation methods (i.e. CEM, CC, Supporting Documents) (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. (B.3)		
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. (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.]
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. (B.3)		
Check that the Certification Body confirms that the Evaluation Facility meets stringent security requirements necessary for the		

Item	Verdict (Y/N/I)	Evidence
protection of sensitive or protected information relating to IT products or Protection Profiles under evaluation and to the process of evaluation itself. (B.3)		
Check that the Licensing or Approval Policy for the Scheme includes details of security and training requirements and of the procedures for making an application to be Licensed or Approved and for the processing of such applications. (B.3)		[Check that the Certification Body includes in its Licensing or Approval policy those requirements that allow it to determine that evaluation facilities have sufficient security measures in place. This also applies for the possibility to determine that the evaluators are technically competent in the field of IT security as well as CC. A mere reference to ISO/IEC 17025 in the Licensing or Approval policy is not sufficient. At the same time it is not expected that the Certification Body has training or examination requirements on a per evaluator basis although this is recommended.]
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. (C.8)		
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 CCRA. 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		

Item	Verdict (Y/N/I)	Evidence
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 procedures for assessing and monitoring their competence; i) details of any procedures for appeals or conciliation. (C.9)		
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. (C.10)		
Check the application of the procedures to ensure the confidentiality of protected information (C.10)		
Check that the Certification Body does not make an unauthorised disclosure of protected information		[Check the Certification Body's procedures to ensure that they help prevent unauthorised disclosures. The VPA team should then ask to

Item	Verdict (Y/N/I)	Evidence
obtained in the course of its certification activities under the CCRA. (C.10)		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. (C.11)		[Check the Certification Body's procedures to ensure that they publish their certified/validated IT product or protection profile on their website and/or the commoncriteriaportal.org website. This is also sufficient to meet the requirement listed in Annex B.2.i. It is not required for the Certification Body to maintain and publish a paper based document. It is allowed for the certificate and Certification Report to be in the national language, although it is recommended for entries on the commoncriteriaportal.org to be in the English language. Note that the Certification Report shall include the Security Target for the IT product, but this Security Target can be sanitized according to the Supporting Document CCDB-2006-04-004]
Check that the Certification Body has procedures to deal with disagreements among itself, its associated evaluation facilities, and their clients. (C.12)		
Check that the Certification Body undertakes management reviews of its operations to ensure that it continues to share the CCRA objectives. (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. (C.14)		

Item	Verdict (Y/N/I)	Evidence
Check that the Certification Body is to have documented procedures for withdrawal of Common Criteria certificates and is to advertise the withdrawal in the next issue of its Certified Products List. (C.15)		