Common Criteria Recognition Arrangement
Management Committee

Operating Procedures

Document Number: 2004-07-01

Date: 7 March 2008

Subject: Conducting Shadow Certifications

Purpose

The purpose of shadow certification is to determine that a Scheme applying for acceptance as a Certificate Producing Nation into the Arrangement on the Recognition of CC Certificates (CCRA) complies with the requirements in Annexes B, C and G of the CCRA.

The focus of the shadow certification program is to ensure that the oversight activities of the Scheme being shadowed meet the CCRA. The principles of certification that are used by the Scheme in overseeing its evaluation facilities should be applied during the shadow certification. There are three phases involved in performing the shadow certification: preparation, site visit, and reporting.

Overview

A team consisting of at least 2 qualified experts; coordinated by the Executive Subcommittee (ES) and approved by the Management Committee (MC), will perform the shadow certification.

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

- Two years as a certifier at a Scheme
- Knowledge of the evaluation facility accreditation process within their own country

It is also highly recommended that the shadow team members have participated in previous shadowing or VPAs either as observers or team members.

The shadow certification activities will be carried out in three phases. The preparation phase will involve review of the Scheme documentation by the members of the shadow team in order to become familiar with the Scheme's policies and procedures. The site visit phase will consist of a one to two-week visit by the shadow team to the Scheme in order to assess the Scheme's technical competence in performing evaluations. This part of the certification will include the review of at least one Scheme evaluation at EAL4. The shadow certification will conclude with the reporting phase.

The shadow team will document their findings and recommendations in a shadow certification report that will be delivered to the ES. The ES will then provide the report to the MC and the MC Chair will notify the Scheme of the final decision.

Scheduling Shadowing Activities

In order to schedule the shadow activity, the Scheme applying for acceptance as a Certificate Producing Nation into the CCRA must send a written application to the Management Committee. The application shall contain a written statement that the applicant Scheme wishes to be determined as compliant under the CCRA and plans:

- To meet all costs of the shadow team whether or not the assessment is successful;
- To provide the documentation listed in Section IV below; and
- To submit two products for review by the shadow team during the site visit that the applicant Scheme has certified.

The Management Committee chairman will acknowledge receipt of the application within two weeks and will forward the application to the Executive Subcommittee for consideration at the next scheduled ES meeting. The ES will provide a response to the applicant Scheme, copying the Management Committee chairman, including a date for the shadow activities (if appropriate) within two weeks of the conclusion of the ES meeting.

Responsibilities of Scheme Being Shadowed

The Scheme is responsible for preparing, documenting and providing general information on at least two EAL3 or EAL4 candidate evaluations. At least one of these must be an EAL4 evaluation. The candidate evaluation information will be provided to the shadow team for their review and selection, within one week, of one of the evaluations for review during the site visit. Although the evaluations 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 evidence has been delivered to and analyzed by the evaluation team.

All written documentation and communications for the shadow 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. The latest issue of the Scheme's Certified/Validated products list;
3. Two or more Common Criteria certificates and Certification/Validation Reports issued under the oversight of the applicant;
4. 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
5. 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 be provided in English.

One part of the shadow 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. This evaluation should be at the EAL4 level. The Scheme is responsible for preparing and documenting general information about at least two candidate evaluations. This candidate project information will be provided to the ES for their review and selection of the projects to be used in the Shadow activities. Although the evaluations 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 evidence has been delivered to and analyzed by the evaluation team.

The candidate project information provided by the Scheme to the ES should include:

- a brief overview of the product,
- the status of the evaluation (if not completed, then indicate what parts of the evaluation have been completed and what remains to be done),

- the target EAL, and
- any Protection Profile compliance claims.

The ES will select the candidate evaluation(s) to be shadowed and will notify the Scheme within one week of receipt of the candidate project information.

The Scheme must have a private room available that is large enough to accommodate the shadow team and Scheme personnel during the site visit. This 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.

The Scheme will identify a point of contact to the ES; who will be the individual responsible for facilitating the shadow activities and for interacting with the shadow team leader and the ES.

The Scheme Point of Contact is responsible for:

- Coordinating the dates of the site visit with the shadow team,
- Delivering the Scheme materials to the shadow team during the Preparation Phase,
- Coordinating all necessary Non Disclosure Agreements with the shadow team prior to the site visit,
- Coordinating the shadow certification agenda for the Scheme, including scheduling certifiers for shadow 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 shadow team during the site visit;
- Providing the shadow 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 shadow certification report by Scheme representatives, and
- Providing feedback to the shadow team leader on the report.

Responsibilities of Shadow Team Leader

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

- Coordinating the receipt of materials from the Scheme,
- Drafting the site visit agenda and coordinating it with the Scheme,
- Coordinating and finalizing the shadow certification report at the end of the site visit,
- Delivering the final shadow certification report to the ES, and if necessary,

- Monitoring the Scheme's resolution of outstanding issues resulting from the shadowing process.

Preparation Phase

The Scheme being shadowed will provide the shadow team with information on at least two candidate evaluations. These candidate evaluations should have been evaluated or be in evaluation at EAL3 or EAL4. At least one of the evaluations should be at the EAL4 level. Those proposed evaluations which have not been completed must have advanced to the point that technical reports and significant evidence have been produced. The shadow team will select one of those proposed evaluations for review during their site visit.

In addition to the two proposed evaluations, the Scheme may also provide the shadow team with information on another two evaluations which were completed in the 12 months prior to the start of the shadow activities. If the shadow team has sufficient time and resources, they will review these evaluations during their site visit and, if they are found to be compliant with CCRA requirements, will permit the Scheme to officially certify these evaluations to receive mutual recognition.

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

The shadow team should begin preparations approximately four weeks prior to the site visit. The Scheme should provide the shadow team with access to all written policies and operating procedure documents. Electronic or hardcopy documentation can be provided, depending on the preference of the shadow team members. The team should focus their review of the documentation on gaining 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, the types of personnel records 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 the technical decisions are recorded and promulgated.

3. Scheme evaluation facilities: how laboratories are accredited and how accreditation is maintained; the role of certifiers in lab assessments.
4. Scheme 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.
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.

The shadow 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 agenda, with input from the team members, at the conclusion of the preparation phase. The agenda must be forwarded to the Scheme no later than one week prior to the commencement of the site visit. It is recommended that the shadow team leader maintain close contact with the Scheme POC during the preparation phase to keep the Scheme apprised of areas that will require further investigation during the site visit.

Site Visit Phase

I. Determine that the constitution and procedures of the Scheme being shadowed comply with the requirements of Annexes B, C and G of the Arrangement on the Recognition of CC certificates (CCRA).

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 and G of the Arrangement on the Recognition of CC certificate (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 EN 45011 or ISO Guide 65 or in accordance with a national interpretation of EN 45011 or ISO Guide 65, then the results of the accreditation may be used in the review of the Scheme's adherence to the requirements of Annex C. The reason for reuse is that the 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.)

If checking the procedures of the Scheme is necessary, this can be accomplished by checking the information required in G.2a of the CCRA according to G.3 of the CCRA.

This check must be completed before the shadow certification process commences. Nevertheless, the shadow 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 shadowed.

II. Perform the shadow certifications.

The shadow 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.

The shadow team shall have access to all evaluation 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 shadow team should observe the meeting. In the event that an evaluation facility will not/cannot permit the shadowing team to visit its facility, the Scheme shall attempt to schedule the meeting at the Scheme facility so the shadow team can observe. The shadow team should not independently review the work of the evaluation facility, which will be covered by EN 45001 or ISO 17025. However, the shadow 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.

The shadow team 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.

a. **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 shadow 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.

b. **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.

c. **Evaluators' technical reports.** 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.

d. **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.

e. **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.

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

g. **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.

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

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

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

During the site visit, the shadow team 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 shadowed (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 shadowed evaluation.

The shadow team should check that all oversight activity is performed in accordance with Scheme procedures and that those procedures are adequate to oversee the evaluation.

At the end of the site visit, the shadow team and the Scheme should agree to the following:

a. a (possibly empty) list of recommendations from the shadow team that record any significant findings,

b. agreement that the recommendations are factually correct; and

c. proposed resolution for the recommendations

If it is not possible to gain agreement on the recommendations, the shadow team should note the disagreement and highlight it in their report.

Reporting

To finalize their work, the shadow team will produce a report that summarizes their findings (see Annex G.4 of the CCRA). The report will be produced during the final day(s) of the site visit and will be coordinated with the Scheme prior to conclusion of the site visit. The shadow team should analyze the impact of any required actions and include these in the shadow certification report. The shadow certification report should be agreed to internally within the shadow team before its submission to the ES. If the shadow team cannot agree internally, then majority and minority opinions should be included in the report.

The shadow certification report shall provide one of four possible recommendations:

• Pass	The Scheme has met all requirements and no further action is required.
• Pass plus recommendations	The Scheme has met all major CCRA requirements, but must implement the recommendations made by the shadow team to be fully compliant.
• Action required before pass	The Scheme must implement recommendations made by the shadow team before they are accepted as a certificate producing nation.
• Reject	The Scheme has not met the requirements and should not be accepted as a certificate producing nation.

The team leader is responsible for delivering the final shadow certification report to the ES within one month of completion of the shadow site visit. The ES will review the report for consistency and soundness of conclusion and will forward it to the MC Chair for review and final approval. 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 ES.

In the case where conditional action 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 shadow team leader and reported to the ES Chair until all actions have been completed. Should difficulties arise, the shadow team leader will facilitate negotiations between the ES Chair, in consultation with the MC, and the Scheme being shadowed. The MC Chair, in consultation with the MC, will be the final arbiter. Upon satisfactory completion of all required actions, the shadow team leader shall notify the ES Chairman and the MC Chairman. The MC Chair shall then notify the Scheme and update the list of CCRA Compliant Certification Bodies accordingly.

In the case of rejection of the Scheme, the MC's response shall provide a summary of the reasons for rejection and the evidence on which the decision is based. In the case of acceptance of the Scheme, the MC Chairman shall update the list of CCRA Compliant Certification Bodies 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 CC certificates (CCRA).

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 and experience and EN45011 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 organization'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 documentation are available at all		[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.]

Item	Verdict (Y/N/I)	Evidence
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)		
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 stored for a period of at least five years. (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		

Item	Verdict (Y/N/I)	Evidence
out in accordance with the applicable IT security evaluation criteria and methods. (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 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 Certification Body		

Item	Verdict (Y/N/I)	Evidence
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 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;		

Item	Verdict (Y/N/I)	Evidence
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 obtained in the course of its certification activities under the CCRA. (C.10)		[Check the Certification Body's procedures to ensure that they help prevent unauthorised disclosures. The shadow 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. (C.11)		
Check that the Certification Body has procedures to deal with disagreements among itself, its associated evaluation facilities, and their clients. (C.12)		

Item	Verdict (Y/N/I)	Evidence
Check that the Certification Body undertakes periodic 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)		
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)		