Common Criteria Recognition Arrangement
Management Committee

Operating Procedures

Document Number: 2002-06-006

Date: June 1st, 2002

Subject: Conducting Shadow Certifications

Purpose

Introduction

The Procedures for voluntary periodic assessments consist of three phases:

- Phase 1: Determine that the constitution and procedures of the Certification Body under assessment comply with the requirements of Annexes C and D of the Arrangement on the Recognition of CC certificates (CCRA).
- Phase 2: Perform the shadow certification
- Phase 3: Prepare the final report and the ES recommendations

Phase 1

Determine that the constitution and procedures of the Certification Body under assessment comply with the requirements of Annexes C and D of the Arrangement on the Recognition of CC certificates (CCRA).

The checklist in Annex A shall be used to determine that the constitution and procedures of the Certification Body under assessment comply with the requirements of Annexes C and D of the Arrangement on the Recognition of CC certificates (CCRA).

This checklist is to be used to determine whether the processes that the Certification Body 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 Methodology. The checklist is applicable to any Certification Body under assessment, although if the Certification Body 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 Certification Body's processes 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 (This standard has been superseded by the 1998 standard, which has added additional requirements.)

When checking the procedures of the Certification Body under assessment, the checking process can be done 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

certification team should check that the Certification Body under assessment is applying its procedures. This can be done at the site visit (see below) for the particular certification body being shadowed.

Phase 2

Perform the shadow certification.

The starting point of the procedures is that a single product has been selected for shadow certification by the Executive Subcommittee from the two products offered (G.3). This product should be in evaluation to EAL3 or EAL4. In practice, it may not be possible to cover all certification activities and a representative sample of certifiers by shadowing one certification. The shadow certification team should select certification activities from different certifications and different certifiers if the Certification Body under assessment, ITSEF and product vendors agree. Certifications which have resulted in a downgrade of assurance or no assurance can be useful to shadow in order to determine how deficiencies in assurance are overseen.

The shadow certification process is not intended to validate the work of the ITSEFs; its scope is limited to a review of the oversight of the ITSEFs by the Certification Body under assessment. Examination of documentation and visits to the Certification Body under assessment should only address the ITSEF's work insofar as it is overseen by the Certification Body. Consequently, the shadow certification team shall have access to all documentation that was used by the Certification Body during the CB's oversight process; and shall be permitted to observe all activities carried out during the CB's oversight process. In the event an ITSEF will not/cannot permit the shadow certification team to visit its facility, the Certification Body shall schedule meetings at the Certification Body facility so the shadow certification team can attend the meetings; the shadow certification team should not independently review the work of the ITSEF, which will be covered by EN 45001 or ISO Guide 25. However, the shadow certification team should assess whether the deliverables available to the Certification Body are of sufficient quality to allow the Certification Body to determine that the evaluations were conducted in accordance with the appropriate methodology.

The shadow certification team shall have access to items of documentation that are commonly available in most CB's oversight activities. These include the following:

a. work programmes supplied by the ITSEF to the Certification Body for the evaluation;

b. copies of all versions of the security target of the product supplied by the ITSEF to the Certification Body for the evaluation;

c. technical reports released by the ITSEF to the Certification Body during the evaluation;

d. evaluation observation reports;

e. review comments on ITSEF output made by the Certification Body relevant to the evaluation;

f. correspondence between the Certification Body and the ITSEF or product vendor/developer regarding the evaluation;

g. the minutes of any meetings held between the Certification Body and the product vendor and/or the ITSEF relevant to the evaluation;

h. the daybooks or other internal technical records kept by the Certification Body relevant to the evaluation; and

i. the certification/validation report for the product. (This should be publicly available).

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

For an ongoing evaluation, not all of the documentation requested may be available. In this case, the shadow certification team should attempt to make up for any deficiencies in documentation during the site visit by requesting access to documentation on another product evaluation. (Any evaluation that was not sufficiently advanced to have generated technical reports and significant Certification Body oversight should not have been accepted by the Management Committee.)

The shadow certification team shall examine all documentation that was used by the Certification Body during the CB's oversight process. Below is a list of documentation, including examination requirements, that is commonly available in most CB's oversight activities.

a. **Evaluator work programs** These should be examined in conjunction with the Certification Body comments and the actual effort figures from the ITSEF (if available) to determine that the Certification Body's oversight ensured that the scope of the evaluation was clearly defined, coherent and conformed with the Common Criteria requirements. The shadow certification team should take into consideration that "evaluators' work programs" is not defined in the CEM so content and scope of work programs may differ between schemes.

b. **Security targets** These should be examined in conjunction with the Certification Body 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. **Evaluator technical reports** These should be examined in conjunction with the Certification Body's comments on the technical reports to determine that the technical reports supply sufficient evidence to demonstrate that the Common Criteria assurance package claimed and reported in the Certification/Validation 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 Certification Body's comments on the observation reports to determine that the Certification Body ensured that the resolution to the observations was adequate.

e. **Certification Body's review comments** These should be reviewed in conjunction with the relevant ITSEF output to determine that they provide effective oversight of the ITSEF output and identify any assurance related deficiencies in that output.

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

g. **Certification Body's internal technical records** These should be reviewed in conjunction with the Certification Body's review comments to determine that all assurance related issues have been assessed adequately.

The documentation review will reveal areas on which the shadow certification team wish to ask questions or raise comments. These comments should be notified in advance of any visit to the Certification Body under assessment in writing (as part of the record of the shadow certification). The Certification Body under assessment may respond in writing to these questions and comments or they can be discussed during

the visit of shadow certification team to the Certification Body under assessment. The shadow certification team may request further evidence for particular areas.

The shadow certification team will arrange at least one visit to the Certification Body under assessment. The visit(s) should be sufficiently long to allow responses to be given by the Certification Body under assessment on all issues about which the shadow certification team has any concerns and to cover all areas listed below. The shadow certification team should plan for a full two weeks of visiting time at the Certification Body site (this may be one or more separate visits) to ensure sufficient time is allotted. If the shadow certification team completes the assessment in a shorter period of time, they need not stay a full two weeks.

During the visit, the shadow certification team should cover areas commonly addressed in most CBs oversight activities. These areas include:

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

b. obtaining an update on the current state of the shadowed evaluation;

c. checking the application of the Certification Body's procedures;

d. observing the Certification Body at meetings with the ITSEF to witness the interaction of the Certification Body, and to confirm that any significant evaluation technical issues are resolved in a satisfactory manner. In the event an ITSEF will not/cannot permit the shadow certification team to visit its facility, the Certification Body shall schedule meetings at the Certification Body facility so the shadow certification team can attend the meetings; and

e. reviewing how the Certification Body resolves problematic or contentious issues relating to the certification of the shadowed evaluation.

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

At the end of the visit(s) the shadow certification team should agree with the Certification Body under assessment the following:

a. a (possibly empty) list of observations from the shadow certification team that record any significant issues of concern to the shadow certification team;

b. agreement that the observations are factually correct; and

c. proposals to resolve the observations.

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

Phase 3

Prepare the final report and the ES recommendations.

To finalize their work, the shadow certification team should produce a report that summarizes their findings (see Annex G.4 of the CCRA).

The shadow certification report should provide one of three possible assessments:

• Pass	The CB has met all requirements and no further action is required.
• Pass plus Recommendations	The CB has met all requirements, but may consider adopting recommendations by the shadow certification team.
• Action required	The CB must undertake identified follow-up action. It may also consider adopting any non-mandatory recommendations.

The shadow certification team should analyse the impact of any actions required, and in conjunction with their organisations' representative on the Executive Subcommittee, they should include in their report a recommendation to the Executive Subcommittee.

Once prepared, a draft copy of the assessment report should be passed to the ES Chair, the Certification Body under assessment, and the Participant of the Certification Body under assessment . The Certification Body under assessment shall have one month to provide comments on the report and negotiate any issues with the shadow certification team. The shadow certification team will then complete a finalized assessment report and a revised recommendation (if necessary) that will then be formally submitted to the ES Chair. The Certification Body under assessment may also submit a statement of clarification to the ES Chair if they consider it to be required.

The assessment report should be agreed internally within the shadow certification team before its submission to the Executive Subcommittee. If the shadow certification team cannot agree internally, then majority and minority opinions should be included in the assessment report.

The ES Chair will distribute the report and any submission by the Certification Body under assessment to all ES members for review. They will have two weeks to review the report and provide comments to the Chair. This should include either endorsement of the shadow certification team's findings, or proposed amendment to either the recommendations or required actions.

Where additional action is required, the CB will be provided with 30 days to propose a resolution to all required actions and 90 days to implement all proposed resolutions. Progress will be monitored by the lead of the shadow certification team and reported to the ES Chair until a pass has been achieved. Where difficulties arise, these will be negotiated between the ES Chair, in consultation with the ES, the Certification Body under assessment, and the Participant of the Certification Body under assessment. The MC Chair, in consultation with the MC, will be the final arbiter.

The ES Chair, in conjunction with the ES members, will have a further two weeks to finalize the report, consulting the shadow certification team and the Certification Body under assessment as appropriate, and submit a copy of the final report to the MC Chair with a recommendation from the ES.

Annex A

Checklist for Determining that the constitution and procedures of the Certification Body under assessment comply with the requirements of Annexes C and D of the Arrangement on the Recognition of CC certificates (CCRA).

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 organisation's personnel department and kept up-to-date. (C.4)		
Check that personnel have available to them clear, up to date, documented instructions pertaining to their duties and responsibilities. (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 this Annex. (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:		[For e, those with a direct interest in the Scheme will include all product vendors who use the Scheme, the ITSEFs and customers of certified products in government departments and companies in the critical national infrastructure. It may also include system

Item	Verdict (Y/N/I)	Evidence
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. (C.5)		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. (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.]
The system is to include 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		

Item	Verdict (Y/N/I)	Evidence
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. (C.7)		
Check that ITSEFs 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 ITSEF. All that is required is that the Certification Body describes how it determines that ITSEFs are technically competent.]
Check that the Certification Body checks to confirm 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 checks to confirm that the Evaluation Facility meets stringent security requirements necessary for the protection of sensitive or protected information relating to IT products or protection profiles		

Item	Verdict (Y/N/I)	Evidence
under evaluation and to the process of evaluation itself. (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. (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 this Annex. 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;		

Item	Verdict (Y/N/I)	Evidence
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 (D)		
Check that the Certification Body does not make an unauthorised disclosure of protected information obtained in the course of its Certification activities under this Arrangement. (C.10)		[Check the Certification Body's procedures to ensure that they help prevent unauthorised disclosures. The shadow certification 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 in published form. Each IT product or protection profile mentioned in the list is to be clearly identified. (C.11)		
Check that the Certification Body		

Item	Verdict (Y/N/I)	Evidence
has procedures to deal with disagreements among itself, its associated ITSEFs, and their clients. (C.12)		
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)		

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