IC3S

Quality Manual

(STQC/CC/D02)

Issue :04

CC Certification Body, STQC Directorate,
Indian Common Criteria Certification Scheme (IC3S),
MeitY, Government of India
INDIA

Table of Contents

Section 0 : Preface

0.1 Introduction

Ministry of Electronics& Information Technology is the nodal agency for all activities related to policy and promotion of IT, internet and E-Commerce. STQC Directorate, as a part of the Ministry, is mandated to align itself w.r.t. the objectives of Ministry and provide support and services to the users in line with these objectives. Over the years STQC's Core Competence has been around Standardisation, Test & Calibration and Certification.

With the Indian IT Act 2008 coming into existence, Ministry has taken up several initiatives to facilitate the spread the use of IT and promotion of E-Commerce. Owing to its Core Competence, STQC is providing IT related services concerning Standardisation, Test & Certification. The "Common Criteria Certification" is one such focused effort on certification.

The Indian Common Criteria Certification Scheme (IC3S) has been set up by the Ministry of Electronics and Information Technology (MeitY) as part of Cyber Security Assurance initiatives of the Government of India. The purpose of the scheme is to evaluate and certify IT Products and Protection profiles (PP) against the requirement of Common Criteria Standards (ISO 15408) at assurance levels EAL 1 through 4. The main beneficiaries of this program are Developer of IT Products or Protection profiles, Sponsors, Common Criteria Test Laboratory (CCTL) and Certification Body. The scheme also provides a framework for the International Mutual Recognition of such certificates with the other member countries of CCRA (Arrangement on the recognition of Common Criteria Certificates in the field of Information Technology).

The Certification Body is the STQC Directorate,Ministry of Electronics and Information Technology (MeitY), Govt. of India.

This document prescribes the operating procedure for the Certification Body as per ISO/IEC 17065 and CCRA Annexure B & C requirements.

0.2 Approval and Issue

Reviewed by : Advisory Board

Approved by : Chairman, Advisory Board

Note:

- Management Representative is responsible for issue and distribution of this document including amendments.
- Holder of this copy is responsible for incorporation of all the amendments and currency of the document.

0.3 Amendment Record

Sl. No.	Date	Issue	Reason for Change/Change Details
1.	01-12-11	01	First Issue
2.	16-10-12	02	Comprehensive review of CC Scheme documentation
3.	27-11-18	03	Comprehensive review of CC Scheme documentation, to align to ISO 17065 requirement, corrective action after Internal Audit
4.	14-06-19	04	Refinement of CCTL and Validators Empanelment processes.

Section 1 : General

1.1 Purpose& Scope

1.1.1 The Certification Body has been established under the official administration procedures of Govt. of India to meet the requirements of ISO/IEC 17065 and CCRA requirements. The IC3S is designed to meet both the intent of the CCRA, and to further the goal of the Government in supporting the trustworthiness of IT products that are part of the national information infrastructure in the public and private sectors. The IC3S is described in the document, Indian Common Criteria Certification Scheme (IC3S), Organization, Management and Concept of Operations (STQC/CC/D01).

1.1.2 This document satisfies the IC3S requirement for a quality manual that includes the procedures demonstrating that the Certification Body complies with the requirements stated in Annex B and C of Arrangement on the Recognition of CC Certification. All Certification Body standard operating procedures are either contained in this document or referenced in other IC3S documents (Master List of Documents). These documents (IC3S) shall be reviewed periodically and updated accordingly. The purpose of this document is to lay down the policies and procedures for IC3S as per the applicable national/international standard or normative documents.

1.1.3 This document describes the organisation of Certification Body and process of certification, which include empanelment of CCTL, by means of assessment and validation provides an adequate level of confidence that the certified product/ protection profile is conforming to the specified requirements of the applicable standard or normative document. It will also ensure consistent and reliable operation of Certification Body thereby facilitating their acceptance on national/international basis in the interest of national /international trade.

1.1.4 This document is applicable to the Certification Body personnel. Others that may find it useful include are CCTL personnel, product developers, and sponsoring organizations.

1.1.5 The term “IT Product” is used generically to represent "Hardware, Software, Firmware or a combination of these”.

1.2 References

ISO/IEC Guide 2	-	Standardization and related activities -- General vocabulary
ISO/IEC 17065	-	General Requirements for Bodies Operating Product Certification Systems
CCRA	-	Arrangement on the Recognition of the Common Criteria Certifications in the Field of Information Technology Security.
ISO/IEC 17025	-	General Requirements for the Competence of Testing and Calibration laboratories.

*(Please refer **Master List of Documents** for latest version of the documents)*

1.3 Definitions

This section contains definitions of terms used in the Indian Common Criteria Certification Scheme (IC3S). These definitions are consistent with the definitions of terms in ISO Guide 2 and also broadly consistent with the Common Criteria and Common Evaluation Methodology. However, the definitions of terms may have been amplified to add greater clarity or to interpret in the context of the evaluations conducted within the scheme.

Accredited: Formally confirmed by an accreditation body as meeting a predetermined standard of impartiality and general technical, methodological, and procedural competence.

Accreditation Body: An independent organization responsible for assessing the performance of other organizations against a recognized standard, and for formally confirming the status of those that meet the standard.

Agreement on the Mutual Recognition of Common Criteria Certificates in the field of IT Security: An agreement in which the Parties (i.e., signatories from participating nations) agree to commit themselves, with respect to IT products and protection profiles, to recognize the Common Criteria certificates which have been issued by any one of them in accordance with the terms of the agreement.

Appeal: The process of taking a complaint to a higher level for resolution.

Approved Lab: Assessed by the Certification Body as technically competent in the specific field of IT security evaluation and formally authorized to carry out evaluations within the context of IC3S.

Approved Laboratories List: The list of approved CCTLs authorized by the Certification Body to conduct IT security evaluations within the IC3S.

Approved Test Methods List: The list of approved test methods maintained by theCertification Body, which can be selected by a CCTL in choosing its scope of accreditation, that is, the types of IT security evaluations that it will be authorized to conduct using approved test methods.

Assurance Maintenance Plan: Part of the formal assurance maintenance documentation submitted to the Certification Body by the sponsor of an evaluation (as part of the initial TOE evaluation) that identifies the plans and procedures a developer

is to implement in order to ensure that the assurance that was established in the validated TOE is maintained as changes are made to the TOE or its environment.

Availability: The prevention of unauthorized withholding of information resources.

Certification: The process carried out by the Certification Body leading to the issue of a Common Criteria certificate.

Certification Report: A publicly available document issued by theCertification Body which summarizes the results of an evaluation and confirms the overall results, (i.e., that the evaluation has been properly carried out, that the Common Criteria, the Common Methodology, and the scheme-specific procedures have been correctly applied and that the conclusions of the evaluation technical report are consistent with the evidence adduced).

Certificate Maintenance Program: A program within the IC3S that allows a sponsor to maintain a Common Criteria certificate by providing a means (through specific assurance maintenance requirements) to ensure that a validated TOE will continue to meet its security target as changes are made to the IT product or its environment.

Certification Agreement: An agreement which is part of the IC3S and which details the mutual rights and obligations of the certificate holder and the Certification Body, and which includes the right to use the certification mark and/or logo and certificate.

Common Criteria (CC): Common Criteria for Information Technology Security Evaluation, the title of a set of documents describing a particular set of IT security evaluation criteria.

Common Methodology (CEM): Common Methodology for Information Technology Security Evaluation, the title of a technical document which describes a particular set of IT security evaluation methods.

Common Criteria Certificate: A brief public document issued by the Certification Body under the authority of STQC which confirms that an IT product or protection profile has successfully completed evaluation by a CCTL. A Common Criteria certificate always has associated with it, a Certification report.

Common Criteria Testing Laboratory (CCTL): Within the context of the IC3S, an IT security evaluation facility, accredited by Certification Body to conduct Common Criteria-based evaluations.

Complaint: A written formal disagreement against a party.

Complainant: The party who makes the complaint.

Confidentiality: The prevention of unauthorized disclosure of information.

Evaluation: The assessment of an IT product against the Common Criteria using the Common Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.

Evaluation Schedule: The schedule established by a CCTL for the conduct of an IT security evaluation.

Evaluation Technical Report: A report giving the details of the findings of an evaluation, submitted by the CCTL to the Certification Body as the principal basis for the Certification report.

Evaluation Work Plan: A document produced by a CCTL detailing the organization, schedule, and planned activities for an IT security evaluation.

Integrity: The prevention of the unauthorized modification of information.

Interpretation: Expert technical judgment, when required, regarding the meaning or method of application of any technical aspect of the Common Criteria and/or Common Methodology.

IT Product: A package of IT hardware, software, and/or firmware providing functionality designed for use or incorporation within a multiplicity of IT systems.

IT System: A group of IT products, either tightly or loosely coupled, working together in a specific configuration to provide a capability or system solution to a consumer in response to a stated need.

IT Security Evaluation Criteria: A compilation of the information which needs to be provided and actions which need to be taken in order to provide grounds for confidence that security evaluations will be carried out effectively and to a consistent standard.

IT Security Evaluation Methodology: A methodology which needs to be used by evaluation facilities in applying IT security evaluation criteria in order to give grounds for confidence that evaluation will be carried out effectively and to a consistent standard.

Logo: A symbol used by a body as a form of identification, usually stylized. A logo may also be a mark.

Mark: A legally registered trade mark or otherwise protected symbol which is issued under the rules of a certification body indicating that adequate confidence is provided that the relevant product, process or service is in conformity with a specific standard or other normative document.

Certification Body: A governmental organization responsible for carrying out Certification and for overseeing the day-to-day operation of IC3S.

Observation Reports: A report issued to the Certification Body by a CCTL or sponsor identifying specific problems or issues related to the conduct of an IT security evaluation.

Party: A signatory to the Agreement on the Mutual Recognition of Common Criteria Certificates in the field of IT Security.

Protection Profile: An implementation-independent set of security requirements for a category of IT products which meet specific consumer needs.

Recognition of Common Criteria Certificates: With respect to the Agreement on the Mutual Recognition of Common Criteria Certificates in the Field of IT Security, acknowledgment by one Party of the validity of the Common Criteria certificates issued by another Party.

Scope of Accreditation: The approved test methods for which a CCTL has been accredited

Security Target: A specification of the security required (both functionality and assurance) in a Target of Evaluation (TOE), used as a baseline for evaluation under the Common Criteria. The security target specifies the security objectives, the threats to those objectives, and any specific security mechanisms that will be employed.

Sponsor: The person or organization that requests a security evaluation of an IT product or protection profile.

Target of Evaluation (TOE): An IT product or group of IT products configured as an IT system and associated documentation that is the subject of a security evaluation under the Common Criteria. Also, a protection profile that is the subject of a security evaluation under the Common Criteria.

Test Method: An evaluation assurance package from the Common Criteria and the associated evaluation methodology for that assurance package from the Common Methodology.

Section 2 : Certification Body –General Requirements

2.1 Legal and contractual matters

2.1.1 Legal Status

I. **Name and Office Locations**

STQC referred as 'Certification Body', operates IC3S Scheme from address as given below:

CC Certification Body, STQC Directorate,
Indian Common Criteria Certification Scheme (IC3S)
Electronics Niketan, 6, CGO Complex,
Lodhi Road, New Delhi – 110003

II. STQC Directorate is a part of Ministry of Electronics& Information Technology (MeitY), Government of India and is legally responsible for all its certification activities. (See Org. Chart, Annexure II)

2.1.2 Certification Agreement

Certification body have a legally enforceable agreement, Certification Agreement describing the rights and duties of applicants and certified clients, including requirements, restriction or limitation on the use of Certification Body's logo.(DocNo. STQC/CC/D14)

2.1.3 Use of Certificates/Licenses and Logos/Marks

a) The Certification Body has procedures (Doc No. STQC/CC/D13) to exercise proper control over ownership, use and display of its certificates/licenses and logos/marks of conformity.

b) If the Certification Body confers the right to use a Logo or Mark to indicate certification of a product/ protection profile the certified organization may use the specified Logo or Mark only as authorized in writing by the Certification Body.

c) The Certification Body will take suitable action to deal with incorrect references to the certification or misleading use of certificates/licenses and logos/marks found in advertisements, catalogues, etc. Such action could include corrective action,

withdrawal of certificate, publication of the transgression and, if necessary, other legal action.

d) The Certificate given to a client under the scheme shall not be regarded as in any way diminishing the mutual contractual responsibilities/obligations between the client and his customer. The issue of certificate does not imply endorsement of an IT product or protection profile by STQC or any other agency of the Indian Governments.

2.2 Management of Impartiality

2.2.1 Certification activities are undertaken impartially,the management of certification body is committed to impartiality

2.2.2 The Certification Body has rights and responsibilities for the impartiality of its certification activities. The Certification Body's personnel along with Head & staff are free from any commercial, financial and other pressures, which might influence the results of the Certification process.

2.2.3 Certification Body identify risks to its impartiality on ongoing basis,this includes the risks arises from its activities, its relationships or relationships of its personnel.

2.2.4 Certification Body has defined documented procedures to minimize or eliminates identified risks to its impartiality.

2.2.5 The Certification Body is not engaged in any activity other than Certification. STQCDirectorate and any part of the same legal entity under its organizational control is not involved in any consultancy activities.

2.2.6 The Certification Body ensures that activities of related bodies do not affect the confidentiality, objectivity or impartiality of its certification. It does not offer or provide:

- Those services that it certifies others to perform
- Consultancy services to obtain or maintain certification
- Services to design/development of IT products/ protection profiles it certifies

2.2.7 The evaluation of product is done by empaneled CCTL and Certification Body ensures that each decision on certification is taken by persons different from those who carried out the Evaluation or Validation.

2.2.8 Certification Body take prompt action to respond to any risks of which it becomes aware to its impartiality, arising from the actions of other persons/organisations/ bodies.

2.3 Liability and financing

2.3.1 The Certification Body has adequate arrangements to cover liabilities arising from its operations and/or activities (in the form of certification agreement).

2.3.2 The Certification Body has financial stability and resources required for the operation of the certification system, in the form of budgetary support from Government of India.

2.4 Non-discriminatory conditions

2.4.1 All the procedures adopted by the Certification Body are administered in a non-discriminatory manner. The Certification Body makes its services accessible to all applicants, without any undue financial or other conditions.

2.4.2 The Certification Body provides unhindered accesswithout any pre-condition to all the applicantsseekingcertification of their IT Product/ protection profiles, whose activities fall within its declared field of operation, without undue financial or other conditions.

2.4.3 The Certification Body confines itsrequirements, validationand review, decisionon certification and surveillance (if applicable)to those matters specifically related to the scope of certification being considered.

2.5 Confidentiality

2.5.1 The Certification Body is legally responsibleand committed, for the management of all information obtainedor createdduring the performanceof certification activities.Except for information that the client makes publicly available, or when agreed between the certification body and the client (e.g. for the purpose of responding to complaints), all other information is considered proprietary and shall

be regarded as confidential. The certification body inform theclient, in advance, of the information it intends to place in the public domain

2.5.2 Except as required in this document information about a particular product or client will not be disclosed to a third party without the written consent of the client. Where the law requires information to be disclosed to a third party, the client will be informed of the information provided as permitted by the law.

2.5.3 Information about the client obtained from sources other than the client (e.g. from the complainant or from the regulator) shall be treated as confidential.

2.6 Publicly available information

The Certification Body, documents, updates &maintains at periodic intervals and makes available, on request, the following

a. Information about the authority under which the Certification Body is operating(Approval of Govt. of India).

b. For certification scheme, a documented statement on the certification scheme incorporating the rules and procedure for granting, maintaining, extending, reducing, suspending and withdrawing certification. (Ref. STQC/CC/D01- CC Scheme Management, Organization and Operations)

c. The Certification Body has financial stability and resources required for the operation of the certification system, in the form of budgetary support from Government of India. The financial administration of the scheme including determination of charges is the responsibility of Head, CC Scheme under the authority of Management. Published schedule of charges (Doc. No. STQC/CC/D07) available to applicants and certified clients.

d. Certification Agreement describing the rights and duties of applicants and certified clients, including requirements, restriction or limitation on the use of Certification Body's logo (Doc No. STQC/CC/D14).

e. The Certification Body has a defined policy and procedure for resolution of Complaints, Appeals and Disputes received from clients or other parties about the handling of certification or any other related matter.

f. Information on procedures for the handling of Complaints, Appeals and Disputes (in the brochures and Certification Agreement and Doc. No. STQC/CC/P07&STQC/CC/P08).

Section 3:Structural requirements

3.1 OrganisationStructure and top Management

3.1.1 The Certification Body has a documented structure which safeguards impartiality, of the operation of Certification Body. It further enables participation of all interested parties in the content and functioning of the certification system.

3.1.2 The Certification Body has an identified management structure which has the overall responsibility for the operation of Certification System. The Organization Chart and the reporting structure is given in Annexure III.

3.1.3 The Certification Body has

a) A Chairman
b) An Advisory Board
c) Management Committee
d) Certification Committee
e) Certification Personnel
    i) Head
    ii) Management Representative
    iii) Validators
    iv) Operations Personnel

TheCriteria, Composition and Terms of Referenceare as below:

a) Chairman, Certification Body

Director General, STQC is the ex-officio chairman of Certification Body acting under the authority of Secretary, Ministry of Electronics and Information Technology, Govt. of India. He is responsible for overall functioning of the 'Indian Common Criteria Certification Scheme (IC3S)' in line with the objectives of STQC Directorate, as well as Ministry.

b) Advisory Board

Objective of Advisory Board

The objective of the Advisory Board isto haveMechanismto safeguard the impartialityof the Certification Operations to provide confidence in certification services provided by the Certification Body.

Structure & Composition of Advisory Board

The Advisory Board will have members not exceeding 15 including the Chairman and Head, CC Scheme.

- DG, STQC is the ex-officio chairman of Advisory Board.
- Members are chosen from among those interested parties involved in the process of certification.
- The members have adequate academic and professional experience in the field of IT Security.
- Knowledge of Common Criteria Standards is desirable.
- In general, the following is deemed as representing the interested parties:

Interested parties

The members from interested parties representing public/ private sector, Government and Professionals are appointed by the Chairman, Certification Body, in consultation with respective interested parties, for a period of 3 years. At the end of the tenure, the Chairman, Certification Body may re-appoint the members for a further period of 3 years. Depending upon the need, the Board may co-opt for more members. In any case, the number of co-opted members will not exceed three and their tenure of membership will not exceed the tenure of the current Advisory Board.

Terms of Reference for Advisory Board

- Formulation of policy matters relating to the operation of Certification Body and approval for adoption of policy related to documentation (Quality Manual), Scheme documents etc.
- Having an overview of the implementation of its policies.
- Setting up of committees as required to which defined activities are delegated or delegate such authority to Management Committee.
- Safeguarding impartiality and enabling participation of all parties concerned regarding the content and functioning of the Certification Body.
- Ensuring that the Certification Body operates in a non discriminatory manner.

The Advisory Board has the power to obtain from the Head, CC Scheme all such information on the conduct of its policy to enable it to discharge its duties properly. The Head, CC Scheme provides all the necessary information, including the reasons for all the significant decisions and actions, and the selection of the persons for a particular activity.

The advice of the board is binding on the Management Committee oncertification related matters.

Business Procedure of Advisory Board

Meetings of the Advisory Board shall be held atleast **once in** a year. The date and place shall normally be decided during the previous meeting. The Chairman of the Advisory Board may at his discretion or at the request of atleast three members call for a special meeting giving prior intimation to the members sufficiently in advance.

The quorum of the meeting is obtained when more than half members are present at the meeting. If there is no quorum, the meeting shall proceed but in such circumstances where decisions require confirmation, voting by correspondence will take place subsequent to the meeting. However, in all cases of voting, the Chairman, Advisory Board and Member Secretary shall not have the right to vote, either in favor or against the matter under consideration for voting.

Depending upon the importance of the matter under consideration during a meeting, the Chairman, Advisory Board may decide for voting at the meeting 8itself or voting by correspondence. The proposal on the subject matter is adopted when no opposing vote is received within the time specified in the correspondence, otherwise, the matter shall be dealt with at the next meeting.

The Certification Body shall maintain records of confidentiality and background experience of the board members.

c) Management Committee

Objective of Management Committee

The objective of the Management Committee is to manage the certification activities in line with the charter of STQC Directorate and advice of Advisory Board.

Structure & Composition of Management Committee

- ***Chairman***

  Head CC Scheme is the ex officio Chairman of Management Committee. Head, CC Scheme is an STQC person of the sufficiently senior level, appointed by Chairman, Certification Body.

- ***Members***

  - Do not exceed 10 in numbers excluding Chairman and Member Secretary,
  - Belong to STQC Directorate of sufficiently senior level, preferably unit/activity head
  - Active professionals in certification related fields, administration & finance
  - The committee shall include representative for each IT certification scheme e.g. (CC Scheme) at least one person with appropriate competence in that field of certification
  - Appointed by Chairman, Certification Body in consultation with Chairman, Management Committee

- Depending on the need the committee may co-opt more members up to a maximum of 2 persons,
- Management Representative is the **member secretary** of the committee.

Terms of Referencefor Management Committee

While being accountable to Advisory Board, the Management Committee will:

- formulate and oversee the implementation of the business plan for Indian CC Certification Scheme.
- decide on approval of decisions made by the Head, CC Scheme and relating to the certification decisions in case of an equal vote in the Certification Committee, or in case the Head, CC Scheme not being in agreement with the advice of Certification Committee,
- provide all requisite information and support to the Advisory Board to enable it to fulfill its obligations,
- ensure compliance with the advice of the Advisory Board,
- carry out periodic reviews of the certification systems/operations to ensure compliance with all applicable requirements,
- seek Advisory Board's concurrence on the technical contents of policy nature for adoption into the certification system,
- set up committees as required to deal with the technical content of the certification system,
- review and approve all scheme specific documentation (except forms / formats),
- make efforts for satisfactory resolution of complaints/disputes received from clients or other parties.

Business Procedure of Management Committee

Meetings of the Management Committee shall be held generally twice a year. A Special meeting of the Management Committee can further be held as and when required by the Chairman or at the request of any of the members.

The business transacted at the meeting shall be recorded in the minutes by Management Representative.

d) Certification Committee

Objective

The objective of the Certification Committee is to advise the Head, CC Scheme on decisions relating to

- Certification of IT Products and Protection Profiles
- Empanelment of laboratories, Certification of evaluators in the empanelled labs.

Structure & Composition of Certification Committee

The composition of the Certification Committee should have competence in auditing/CC validation and subject expertise, represented by one or more persons individually or collectively.

- Have adequate academic background or experience in Information Technology and Infrastructure related issues.
- Involved/engaged in IT/IT Security related projects/activities.

Chairman, Certification Body shall appoint members of the Certification Committee.

Terms of Reference for Certification Committee

While advising the Head, CC Scheme on certification related decisions, the Certification Committee will:

- ensure compliance of evaluation and validation to the defined criteria
- review the reports for adequacy of their content
- provide feedback for improvement
- seek expert opinion where necessary for determining the technical basis for granting certification,

While advising on technical interpretation to various committees, they are required to be:

- independent in opinion
- confidential
- impartial
- objective
- technologicalrelevant etc.
- accountable to the committees

Business Procedure of Certification Committee

The committee shall normally meet once in a fortnight or as required. The independence of the committee in each decision shall be ensured by not involving committee members who took part in the validation process on which a decision has to be made. The minimum quorum of the committee should consist of atleast three independent members. If excluding one or more committee members should result in inappropriate expertise, being present while needed to make a certification decision, the convener shall arrange for the participation of independent experts during the relevant parts of the meeting.

The Convener is not a party to the decision of the committee.

The convener of the committee presents all requisite information along with supporting documentation to the committee. The committee will examine the inputs and advises the Head, CC Scheme on certification decision.

The Committee shall not normally overturn a negative recommendation of the validation team. If such a situation should arise, the Certification Committee shall document and justify the basis for the decision to overturn the recommendation and seek clarification whenever required.

e) Certification Operations Personnel

i) **Head, CC Scheme**

- is an active professional in QA, belonging to STQC Directorate and of the sufficiently senior level.
- has sufficient work experience (preferably not less than 10 years) in certification and accreditation matters.
- meets qualifications and criteria of a Validators, lead assessor in ISMS etc.
- Knowledge of CC standards
- Qualified Evaluator/validator of the scheme
- is appointed by Chairman, Certification Body.
- Along with his team (certification personnel) is responsiblethereby to the Advisory Board for day to day operation of the Certification System.
- will act on the advice of Certification Committee on certification decisions. In case of equal votes, the Certification Committee or conflictof opinion with the decision of the Certification Committee, he may take a decision.
- is the member secretary of the Advisory Board.
- is responsible for approval of Documents/ Procedures and Forms/ Formats.

ii) **Management Representative (MR)**

The Management Representative is a person, appointed by Chairman, Advisory Board having

- Adequate academic qualifications (preferably a Science/Engineering graduate) with adequate knowledge in Information Technology
- QA experience of atleast 10 years
- Training, qualification and experience of a Management System Lead Assessor, Common Criteria and other IT security standards
- Knowledge and awareness of matters related to Certification and Accreditation

Responsibilities of Management Representative

- To ensure that a system is established, implemented and maintained in accordance with this document
- To report on performance of the system to the management committee of the Certification Body for review and as a basis for improvement

iii) **Validator**

- The policies and procedures for the recruitment & training of Validators /specialists and monitoring of their performance are described in the scheme specific document.
- Responsible for carrying out their assigned activities on the advice of Certification Body.
- Clearly documented procedures/instructions are available for carrying out assigned activities.
- Records of training, experience and background information of individual validators/specialists are maintained.

iv) **Operations Personnel**

- The personnel looking after the certification operation of the Certification Body.
- are having adequate academic background (preferably Graduate/Diploma in Engineering or Science graduate)
- having sufficient work experience (preferably not less than 2 years) in Quality Assurance,Information Technology and Information Security.
- preferably meet training & qualification related to relevant scheme and criteria.
- are responsible for day-to-day operations, all liaison/co-ordination within and outside the certification body.
- have adequate procedure and instructions/guidelines for carrying out their activities related to:

    - maintenance of files, records and website related to certification matters.
    - support to Certification Personnel
    - Maintenance of the database.

3.1.4 The Certification Body has defined criteria for appointment and operation of all the committees needed for the Certification process. These committees are free from any commercial, financial and other pressures that might influence decisions.Certification body retains authority to appoint and withdraw members of such committees.

3.1.5 List of Appointments

The document, STQC/CC/D11 – "List of Appointments" identifies the personnel &other resources involved in the activities of Certification Body as follows:

- Members of Advisory Board
- Members of Management Committee
- Head, CC Scheme
- Members of Certification Committee
- Management Representative
- Validators
- Certification Operations personnel

The responsibilities of all personnel involved in the certification activities are indicated in the document,STQC/CC/D12- "Responsibility Matrix".

3.2 Mechanism for safeguarding impartiality

Refer 3.1.4 b) Advisory board - objective, terms of reference & business procedure.

Section4: Resource Requirements

4.1 Certification Body personnel

4.1.1 General

4.1.1.1 The Certification Body has a sufficient number of personnel having the necessary education, training, technical knowledge and experience for performing certification functions under the overall responsibility of Head. These personals are free from any commercial, financial and other pressures that might influence decisions.

4.1.1.2 The personnel of the Certification Body involved in certification shall be competent for the functions they perform, such as:

a. Review of contracts with the clients (application handling)
b. Select and verify the competence of validators
c. Brief validators and arrange any necessary training
d. Decide on the granting & maintaining certification
e. Set up and operate appeals/complaints procedure

4.1.1.3 The certification body has adequate arrangements, consistent with applicable laws, to safeguard confidentiality of all information obtained or created in the course of certification activities at all levels of its organizations, including committees and external bodies or individuals acting on its behalf. All the personnel, except, officials of Ministry of Electronics& Information Technology (MeitY),involved in certification activities as members of the various committees and Board are required to sign a Confidentiality Statement (Form No. STQC/CC/F07), to safeguard confidentiality of the information obtained during their association with certification activities. Ministry officials are already bound by the Code of Confidentiality with Government of India at the time of appointment.

4.1.2 Management of Competence of CB personnel

4.1.2.1 Information on the relevant qualifications, training and experience of each member of the personnel involved in the certification process is maintained by the Certification Body. Records of training and experience are kept up-to-date.

4.1.2.2 Clearly documented instructions are available to the personnel describing their duties andresponsibilities. These instructions are maintained up-to-date.

4.1.2.3 Assessment / Personnel Records

The Certification Body shall possess and maintain up-to-date records on validators consisting of:

a) Name and address
b) Affiliation and position held in the organization
c) Educational qualification and professional status
d) Experience and training in each field of competence of the certification body
e) Date of most recent updating of record
f) Performance appraisal
g) Area of Technical Expertise

4.1.3 Contract with the personnel

The Certification Body requires all the personnel involved in the validation to sign a 1contract by which they commit themselves to comply with the rules defined by the Certification Body, including those relating to confidentiality and those relating to independence from commercial and other interests and any prior and/or present link with the clients or products or protection profiles to be validated.

Certification bodies shall use this information as input into identifying risks to impartiality raised by the activities of such personnel. or by the organizations that employ them.

4.2 Resource for Evaluation

4.2.1 Qualification Criteria for Validators

4.2.1.1 In order to ensure that validations are carried out effectively and uniformly, the minimum relevant criteria for competence is defined by the Certification Body.

4.2.1.2 The qualification criteria for Validators for certification scheme has been defined separately in the document STQC/CC/D17-"Qualification Criteria for Validators"

4.2.2 Validator Selection Procedure

The Certification Body has a procedure (Doc. No. STQC/CC/P01) for selection of validators.

a) selecting validators, on the basis of their competence, training, qualifications and experience;

b) initially assessing the conduct of validators

c) (if required) during validations and subsequently monitoring their performance.

4.2.3 Assignment for a Specific validation

When selecting validator(s) for a specific validation assignment the Certification Bodyshallensure that the skills of the validator(s) are appropriate and the validator(s) are:

a) familiar with the applicable legal regulations, certification procedures and certification requirements.

b) have a thorough knowledge of the relevant validation methodologies and documents

c) have appropriate technical knowledge of the specific activities for which certification is sought and where relevant, with associated procedures and their potential for failure.

d) have a degree of understanding sufficient to make a reliable validation of the compliance of the products with CC standards.

e) areable to communicate effectively, both in writing and orally in the required languages

f) arefree from any interest that might cause team members to act in other than an impartial or non-discriminatory manner i.e.

- Validators or their organization shall not have provided consulting services to the applicant or certified organization which might compromise the certification process and decisions
- In accordance with the directives of the Certification Body, the validators shall inform the Certification Body, prior to the validation, about any existing, former and envisaged link between themselves or their organizations and the applicant organization.

The requirement for specific validation assignment has been defined in STQC/CC/P01. Technical Oversight process has been defined in STQC/CC/D08 and STQC/CC/D09.

4.2.4 Training

Training to facilitate continuing Professional skill development shall be conducted as per Doc. No.STQC/CC/P02 – "training".

4.2.5 Procedures for updating Validators

Validators shall be provided with up-to-date instructions and all relevant information on certification arrangements and procedures.

4.3 Out sourcing/ Sub-Contracting

Presently, subcontracting of the certification related work is not done.

Section 5 : Process Requirements for Certification

5.1 General Information

5.1.1 A detailed description of the certification procedures and the documents containing the requirements for certified IT Products and protection profiles are maintained up-to-date as specified in Cl. No. 2.6 These are provided to applicants.

5.1.2 The Certification Body requires that an Applicant:

a) always complies with the relevant provisions of the certification site visit programme.

b) make all necessary arrangements for the conduct of evaluation and validation, including provision for examining documentation and the access to all areas, records (including internal audit reports) and personnel for the purposes of the site visit and resolution of complaints.

c) only claims that it is certified with respect to those products/PPs for which it has been granted certification

d) does not use its certification in such a manner so as to bring the Certification Body into disrepute and does not make any statement regarding its certification which the Certification Body may consider misleading or unauthorized

e) upon suspension or withdrawal of its certification (however determined) discontinues use of all advertising matter that contains any reference thereto and returns any certification documents as required by the Certification Body

f) uses certification only to indicate that the PP or product is in conformity with specified standards or other normative documents, and does not use its certification to imply otherwise

g) ensures that no certification document, mark or report nor any part thereof is used in a misleading manner

5.1.3 The Certification Body has defined criteria (covered under scheme specific documentation) against which the IT product/ protection profile of an applicant is evaluated and certified.

5.1.4 If requested, additional application information is provided to the applicant.

5.2 The Application

5.2.1 The Certification Body requires an official Application Form duly completed, and signed by a duly authorized representative of the applicant, in which or attached to which

a) the scope of the desired IT Product/ Protection Profile certification is defined
b) the applicant agrees to comply with the requirements for certification and to supply any information needed for its evaluation.
c) EAL Level (augmentation, if any).
d) Security Target Document and other documents as applicable to the IT Product/Protection Profile.

5.2.2 Detailed instructions on application handling are covered in Doc No. STQC/CC/P09.

5.3 Application Review

5.3.1 Before proceeding,the Certification Body will conduct, and maintain records of a review of the request for certification to ensure that

a) the requirements for certification are clearly defined, documented and understood

b) any difference in understanding between the Certification Body and the applicant is resolved.

c) the Certification Body has the capability and means to perform the certification service in respect to the scope of the certification sought, any special requirements such as the language used by the applicant.

d) In case certification body uses information of previously granted certificate , it shall refer the same in the records of evaluation /certification under consideration including its justification for omission of activity if any through impact analysis. ReferSTQC/CC/D10

A Certification Agreement in Doc No. STQC/CC/D14 is entered into with the applicant. The multi sites manufacturing and delivery centers are identified for site visit requirement, if needed.

5.4 Evaluation

(a) Empanelment of CCTL:

5.4.1 The evaluation activities shall be conducted at the CCTL, established either under the provision of Govt. official administrative procedure or through the process of accreditation of CCTL under IC3S. The CCTL shall be technically competent in the specific field of IT security evaluation and shall have a management structure including a Head, Quality Manager and at least two Evaluators. It shall have to comply with the requirementsspecified in the scheme. The accreditation process of CCTL and the requirements for the CCTLs have been defined in the documents, STQC/CC/D03- "Accreditation process for empanelment and operation of labs under IC3S" and STQC/CC/D04 – "Requirements for Test Laboratories" respectively.

(b) Evaluation of Product:

5.4.2 The Certification Body will appoint the CC Test Laboratory to allow for the necessary arrangements for evaluation as per the competency and scope of approval.

5.4.3 The Certification Body will nominate a qualified validator to evaluate.

5.4.4 The client will be informed of the name of the CCTL who will carry out the evaluation with sufficient notice to appeal against the appointment of any particular CCTL.

5.4.5 The CCTL will be formally appointed and provided with the appropriate working documents. The plan for and the date of the evaluation will be agreed between the applicant and CCTL.

5.4.6 Detailed procedure on Technical oversight of IT Product (TOE Evaluation) and Protection Profiles covered in Doc.No. STQC/CC/D08andSTQC/CC/D09 respectively.

5.4.7 The CCTL shall perform evaluation of the Product /PP and site visit as per the requirements of the CC standard. The CCTL shall issue evaluation reports of its work (e.g. site visit report, independent test report, VA report and ETR) that accurately, clearly, and unambiguously present the evaluator analysis, test conditions, test setup, test and evaluation results, and all other required information.

5.5 Evaluation Technical Report (ETR)& Review

5.5.1 The CCTL shallformally report the results of the evaluation task to the CB for approval in the Evaluation Technical Report (ETR).

5.5.2 The ETR shall present all verdicts, justifications and findings derived during the evaluation activity.

5.5.3 The CB ensures that the contents of the ETR comply with requirements specified in the CCRA document (Ref. Section 1.2).

5.5.4 Initially, the CCTL shall mark evaluation results as “Confidential” for distribution only to the CB.

5.5.5 The CCTL is able to distribute a sanitised version of the evaluation results to interested government agencies when CB has approved the results of the evaluation.

5.5.6 The CCTL shallinclude the following major areas within the ETR for product evaluations:

- Executive summary
- Introduction
- Product description (to include an overview, usage and environmental assumptions), threats, organisational security policies and a clarification of scope
- The evaluation context, including the evaluated configuration, security policy, product architecture and testing efforts
- Evaluation results
- Product delivery and installation
- Conclusions and recommendations
- Evaluation documentation
- Problem reports and resolutions.

5.5.7 The certification body has reporting procedures, which will ensure that

a) the validator provides the Certification Body with a report of its findings as to the conformity of the client’s system with all of the certification requirements.

b) a report on the outcome of the certification is promptly brought to the client’s attention by the Certification Body, identifying any non-conformity to be discharged in order to comply with all of the certification requirements and the extent of any further assessment required.

5.5.8 The certification body review all information and results related to the evaluation, the review is carried out by person different than involved in evaluation process.The recommendations for a certification decision based on the review is documented.

5.6 Decision on Certification

5.6.1 The decision whether or not to certify a client's system will be taken by the Head, CC Scheme based on the recommendation of the Certification Committee on the basis of the information gathered during the certification process and any other relevant information.

5.6.2 The Certification Body will not delegate authority for granting, maintaining, extending, reducing, suspending or withdrawing certification to an outside person or body.

5.7 Certification Documentation

The Certification Body will provide to each of its clients whose products/ protection profiles it certifies, a certificate (STQC/CC/F10) signed by Head, CC Scheme or an officer who has been assigned such responsibility. The CB ensures that the content of the certificate complies with the requirements specified in Annex J of the CCRA document. The certificate shall include the following details:

- Product vendor name;
- Product name;
- Product type;
- Version and release numbers;
- Protection Profile conformance (if applicable);
- Evaluation platform (optional);
- CCTL name (optional);
- The IT security evaluation criteria that was used
- Certificate number;
- Date issued; and
- Evaluation Assurance Level (EAL) including any augmentations.

5.7.1 Certification Report

The contents of CR shall comply with the requirements specified in Annex I of CCRA document. The CR shall contain:

a) Report identification details

The details shall include as a minimum,

- Date(s) of report
- Names of the person(s) responsible for the report
- Names and addresses of all sites visited for assessment
- Scope of certification or reference thereto including reference to the standard applied and EAL

b) Evaluation details

For Product evaluations, the details shall include the followingmajor areas:

- An executive summary;
- A section identifying the evaluated IT product;
- A description of the IT product's security policy;
- Assumptions and clarification of scope in relation to the evaluation;
- Architectural information for the evaluated IT product;
- A description of the testing effort performed during the evaluation;
- A description of the evaluated configuration;
- The results of the evaluation;
- Certifier comments and/or recommendations;
- Annexes, including a glossary and/or bibliography if required; and
- Reference to the complete and sanitised version of the ST for the evaluated product. A sanitised version means that commercially sensitive information has been removed from the ST.

5.5.3 Detailed procedure on CC validation is covered in Doc No. STQC/CC/D08andSTQC/CC/D09.

5.8 Directory of certified products

Simultaneously, arrangements will be made to update the list of certified product list (STQC/CC/F11)

5.9 Surveillance

5.9.1 Where ever surveillance is required by the certification scheme, the certification body Plan & conduct surveillance of the product(s), process or service covered by the certification decision in accordance with the certification scheme. (Marking on product/packaging is not applicable under this scheme).

5.9.2 When surveillance utilizes evaluation, review or a certification decision, the compliance to respective requirements, shall be taken care of.

5.10 Changes in the Certification Requirements

5.10.1 The Certification Body will give due notice of any changes it intends to make in its requirements for certification. It will take account of views expressed by the interested parties before deciding on the precise form and effective date of the changes. Following a decision on, and publication of, the changed requirements it shall verify that each certified client carries out any necessary adjustments to its procedures within such time, as in the opinion of the Certification Body, is reasonable.

5.10.2 The CB shall maintainand re-evaluate the Certification, in case of changes to a certified product, through an impact assessment as defined in the document, STQC/CC/D10 – "Assurance Continuity Guidance".

5.11 Termination, Reduction, Suspension or Withdrawal of Certification

5.11.1 The Certification Body is responsible for its decisions relating to the granting, maintaining, extending, reducing, suspending and withdrawing of the certificationsunder the following circumstances

- if the client either will not or cannot ensure conformance to changed rules of procedure of Certification Body
- When a nonconformity is substantiated, either as a result of surveillance or otherwise
- if the client ceases to supply the product
- if the client fails to meet the financial obligation to Certification Body at the formal request of the client
- in case of any other serious contravention of applicable requirements of rules or procedures defined by the Certification Body

5.11.2 Certification body will take actions as specified in the certification scheme, if certification is terminated (including on request of the client), suspended or withdrawn. After suspension, take actions (on request of client or as per policy of certification scheme) needed to end suspension and restore certification for the product(s) based on outcome of certification decision.

5.11.3 In case of certification is terminated, suspended, withdrawn or scope is reduced The certification body makes all necessary modifications to formal certification documents, public information, authorizations for use of marks, etc., in order to ensure all appropriate indications and provide clear and updated information to all interested parties.The certified product list shall be updated accordingly.

5.12 Records

5.12.1 The Certification Body maintains a record system to comply with existing regulations. The records demonstrate that the certification procedures have been effectively fulfilled, particularly with respect to application forms, assessment reports, and other documents relating to granting, maintaining, extending, reducing, suspending or withdrawing certification. The records are identified, managed and disposed of in such a way as to ensure the integrity of the process and confidentiality of the information.

5.12.2 The Certification Body has procedures (Doc. No.STQC/CC/P06) for retaining records for a period consistent with its contractual, legal or other obligations. Access to these records is consistent with the confidentiality requirement of this document.

5.12.3 As far as possible the evaluation evidences shall be maintained in electronic form. Whenever the evidences are in paper form, those shall be scanned and archived and the papers shall be disposed off through shredding on closure of the project.

5.13 Appeals, Complaints and Disputes

5.13.1 Appeals, Complaints and Disputes brought before the Certification Body by Applicant/Certified organization or other parties are subject to the procedures of the Certification Body as below :

Appeal procedure	-	Doc. No. STQC/CC/P07
Complaints/Disputes	-	Doc. No.STQC/CC/P08

5.13.2 The Certification Body shall

a) Keep record of all appeals, complaints and disputes and remedial actions relative to certification

b) Take appropriate corrective and preventive action

c) Document the actions taken and assess their effectiveness.

5.13.3 Access to Records of Complaints

The Certification Body shall require the certified organization to

a) keep a record of all complaints made known to the client relating to product's compliance with applicable requirements and to make these records available to the Certification Body when requested

b) Take appropriate action with respect to such complaints and any deficiencies found in products that affect compliance with the requirements for certification

c) Document the actions taken.

Section 6: Management system requirements

6.1 Certification Policy and Objectives

6.1.1 Goal

To provide services for Common Criteria certification of IT products and protection profiles in a consistent, competent, credible and reliable manner thereby facilitating their acceptance on a national/international basis in the interest of trade.

6.1.2 Certification Policy

To continuously improve and sustain the quality of IC3S services, consistent with market requirements and technological developments to provide better value to the clients.

6.1.3 Certification Objectives

The certification body seeks to achieve its organizational goal by following means:

- Establishing a system in line with internationally accepted norms (e.g. ISO/IEC Standards, CCRA requirements)
- Empanelment of CCTL
- Certifying IT products / protection profiles as per applicable norms
- Continuously reviewing and upgrading technical content of the activities in line with market need
- Seeking strategic alliances with other national/international agencies engaged in similar work
- Adopting innovative methods/practices to provide better value to the clients

The management is committed to ensure that the policy is understood, implemented and maintained at all the levels of the certification body through regular interactions.

To be in line with the policies and objectives the management committee of IC3S will determine, on a regular basis, the need for specific objectives and pursue their compliance.

6.2 General management system documentation

6.2.1 The Certification Body has a documented system defining its policy, including objectives and its commitment. The Certification Body ensures effective implementation of documented system procedures. The structure of the system documentation is as given at Annexure I. The following paragraph identifies the broad contents of various categories of documentation.

- **Quality Manual**
  - Certification policies and objectives as per the requirements of ISO/IEC 17065 and CCRA Annexure B & Crequirements
  - Adequate references to specific Procedures
  - Process flow (Certification)
- **Documents/ Procedures**
  - Details about certification system elements as applicable to IC3S (e.g.Internal Audit, Management Review, Doc. Control etc.).

6.2.2 The Management Representative is a person, appointed by Chairman, Advisory Board who, irrespective of other responsibilities, have responsibility and authority that includes;

- To ensure that a system is established, implemented and maintained in accordance with this document
- To report on performance of the system to the management committee of the Certification Body for review and as a basis for improvement

6.2.3 All personnel involved in certification activities shall have access to the parts of the management system documentation and related information that are applicable to their responsibilities.

6.3 Control of Document

6.3.1 The Certification Body has established and is maintaining procedures to control all documents and data that relate to its certification functions. (The documentation structure is given in para 2.5.3 of this document). These documents are reviewed and approved for adequacy by authorised and competent personnel prior to issue (either on initial development/or any subsequent amendment). The following table identifies reviewing and approving authorities for various types of documents within the system : (2.8.1)

Sl. No.	Documents	Review Authority	Approval Authority
1.	Quality Manual, Scheme	Advisory Board (AB)	Chairman, AB
2.	System procedures/forms	Management Representative (MR)	Head, CC Scheme

6.3.2 A Master list of documents identifying the current revision of documents (Internal and External) shall be maintained. The distribution of all these documents shall be controlled to ensure that appropriate documentation is made available to personnel of certification body or client when required to perform any function relating to the activities of an applicant or the certified client.

6.3.3 The Certification Body has a documented management system to provide confidence in its ability to operate a certification system.

6.3.4 Detailed procedure for document control is described in the document, STQC/CC/P05- "Document Control".

6.3.5 MR shall be the custodianof all external documents e.g. CC standards, interpretations, reference material, etc. and shall be responsible for regular update of the documents of the external origin, the others can be referred on a need basis.

6.3.6 Information on procedures for the handling of Complaints, Appeals and Disputes (in the brochures and Certification Agreement and Doc. No. STQC/CC/P07&STQC/CC/P08.Updated list of Certified Product List Ref. STQC/CC/D15shall be maintained.

6.4 Control of records

6.4.1 The certification body shall establish procedures to define the controls needed for the identification, storage, protection, retrieval, retention time and disposition of its records related to the fulfillment of this International Standard.

6.4.2 The certification body shall establish procedures for retaining records for a period consistent with its contractual and legal obligations. Access to these records shall be consistent with the confidentiality arrangements.

6.5 Internal audits

6.5.1 For the purpose of verifying that the system is implemented and effective, Internal Audits shall be carried out covering all procedures in a planned and systematic manner.

6.5.2 Audits shall be conducted by trained personnel independent of the area/activity being audited.

6.5.3 It shall be ensured that

- Personnel responsible for the area audited are informed of the outcome of the audit.
- Corrective action is taken in a timely and appropriate manner.
- Opportunities for improvements are identified.
- Results of the audit are recorded for periodic review.

6.5.4 Internal audits of the entire system will be carried out at least once a year.

6.5.5 Detailed procedures for carrying out internal audits are covered in the Document, STQC/CC/P03-"Internal Audit".

6.6 Management Review

6.6.1 Management reviews shall be conducted at least once in a yearto ensure continuing suitability and effectiveness of the Certification system.

6.6.2 Management Review includes assessment of the results of Internal Audits, Appeals,Complaints etc., details are in procedure.

6.6.3 The Management Reviews are conducted by the Management Committee.

6.6.4 Records of the reviews are maintained by the Management Representative.

6.6.5 Detailed proceedings for conducting Management Review are covered in the document, STQC/CC/P04- "Management Review".

6.6.6 Review outputs

The outputs from the management review shall include decisions and actions related to the following:

a) improvement of the effectiveness of the management system and its processes;

b) improvement of the certification body related to the fulfillment of this International Standard; c) resource needs.

6.7 Non-conformity Handling and Corrective/Preventive Action

6.7.1 The Certification Body will ensure that any non-conformity detected/reported at any stage of certification activities by anyone, is removed/cleared at the earliest possible time. The control of non-conformance involves

* Identification
* Documentation
* Evaluationfor determining the cause of nonconformity & need for actions
* Segregation (where practical)
* Disposition of non-conformance to ensure that nonconformities do not recur
* Recording the results of actions taken
* Notification to all concerned.

6.7.2 The following identifies the responsibility for review and authority for disposition of non-conformances

Sl. No.	Type of Non-conformance	Review Responsibility	DispositionAuthority
i)	Quality System Documentation related :		
	- Non policy issues	ManagementRepresentative	Head, CC Scheme
	- Policy issues	Head, CC Scheme	ManagementCommittee
ii)	Certification operations related	Operations Personnel	Head, CC Scheme

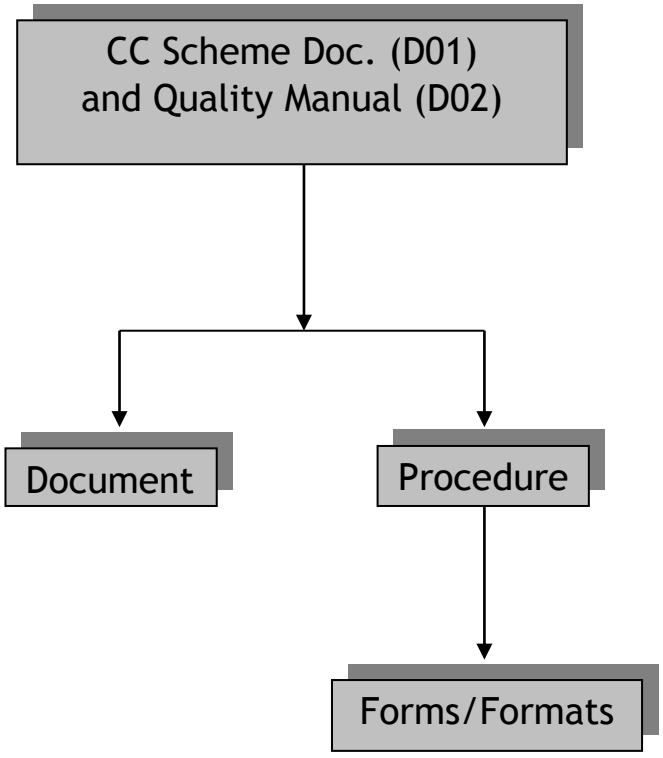
6.7.3 Any non-conformity detected within the system shall be reported to identified authorities as in Cl. 2.11.2 above for review and disposal action. Customer complaints and audits related to non-conformances are reported to Management Representative (MR) who in turn will notify concerned authorities for review and disposal action.

6.7.4 Head, CC Scheme shall be responsible for disposal of any un-resolved non-conformances.

6.7.5 Identified authorities for disposal action as in 2.11.2 above shall be responsible for initiating adequate and appropriate corrective/preventive action commensurate with the magnitude of the problems and levels of risks. Any changes to the procedures/practices are recorded and implemented.

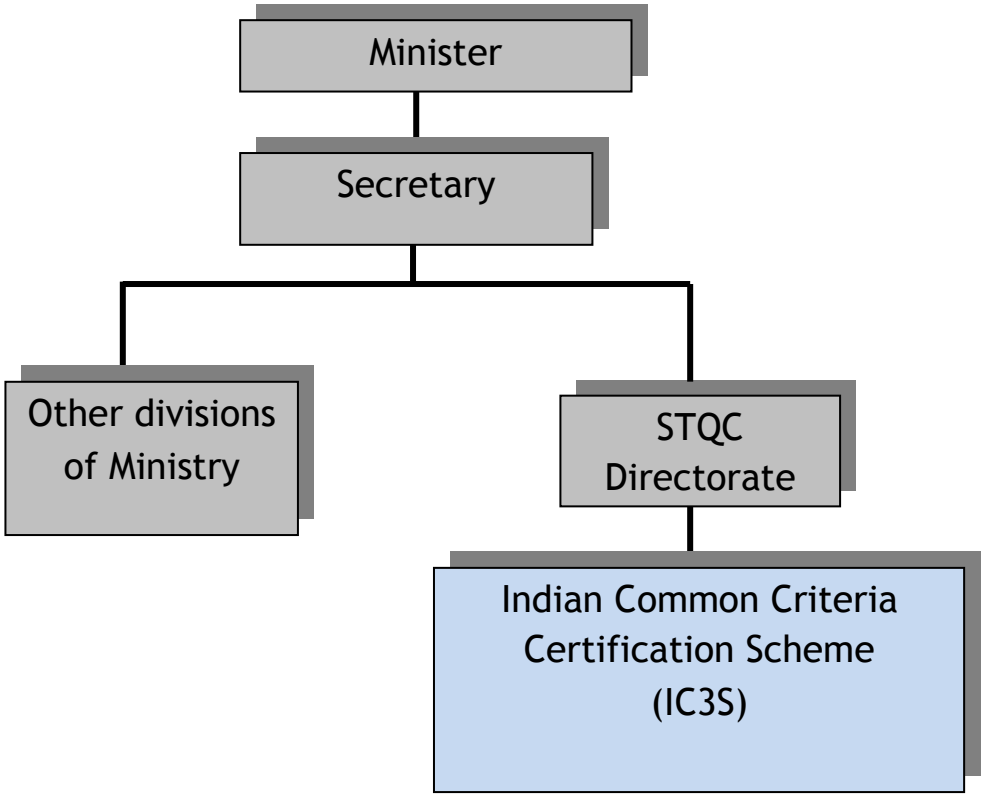
6.7.6 Certification Body shall ensure that identified corrective/preventive actions are taken, as defined in STQC/CC/P10 – "CA/PA Procedure" and those are effective. Relevant information on the actions are submitted for management review.

Annexure-I :IC3S Documentation Structure

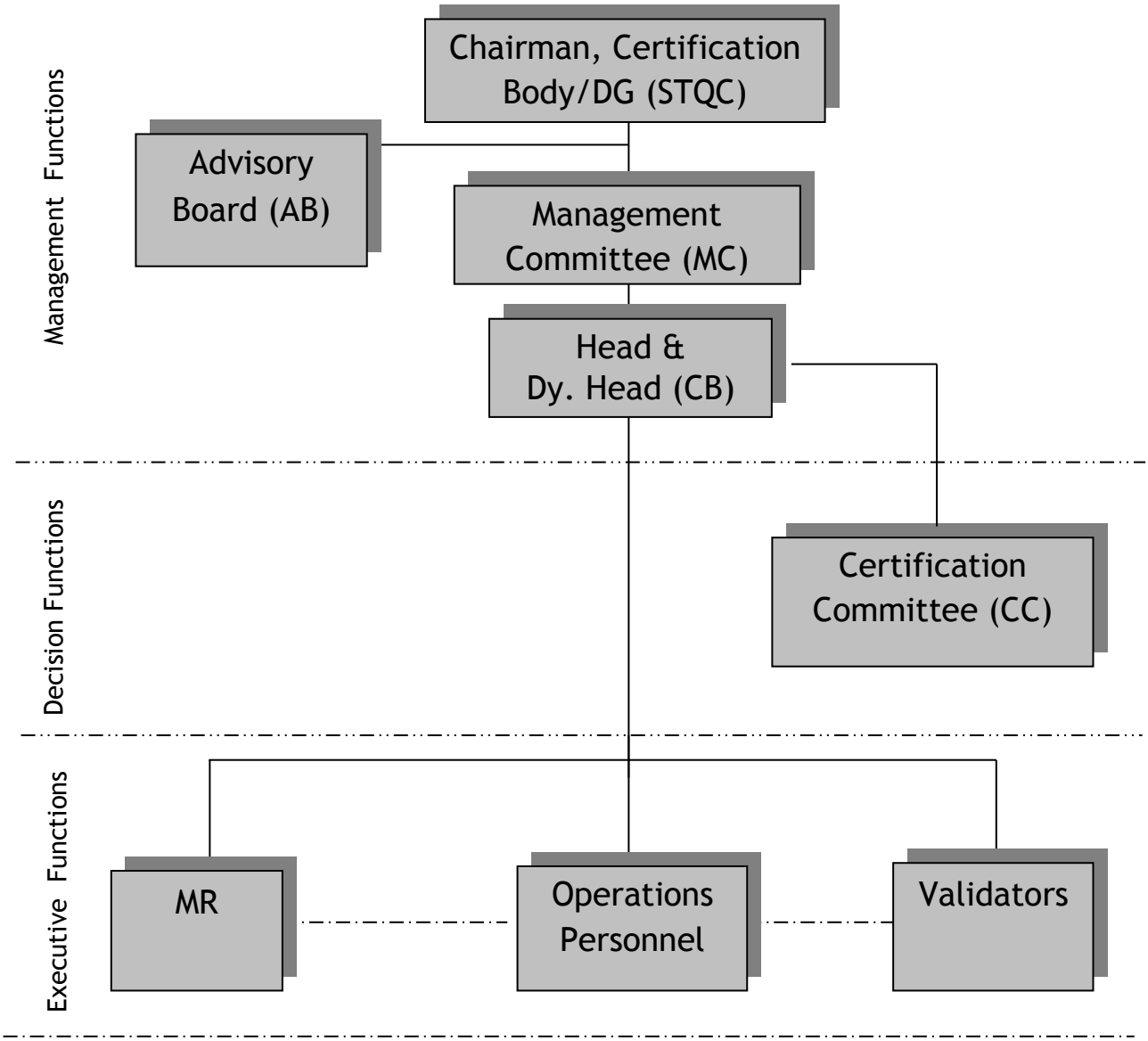


Note: For details refer Master list of documents (STQC/CC/F09)

Annexure-II:Reporting Structure of CC Certification Scheme



Annexure-III :Functional Organisation Structure of STQCCC Certification Scheme



Annexure-IV: Compliance to ISO/IEC 17065

CROSS REFERENCE ISO/IEC 17065 and Quality Manual

SL. No.	ISO / IEC 17065:2012	Title of clause	Corresponding clause of the Quality Manual
1.	4	General Requirements	Section 2
2.	4.1 4.1.1 4.1.2 4.1.3	Legal and contractual matters Legal responsibility Certificate agreement Use of license, certificate and marks of conformity	2.1 2.1.1 2.1.2 2.1.3
3.	4.2	Management of impartiality	2.2
4.	4.3	Liability and financing	2.3
5.	4.4	Non-discriminatory conditions	2.4
6.	4.5	Confidentiality	2.5
7.	4.6	Publicly available information	2.6
8.	5	Structural requirements	Section 3
9.	5.1	Organisational structure and top management	3.1
10.	5.2	Mechanism for safeguarding impartiality	3.2
11.	6.	Resource requirements	Section 4
12.	6.1 6.1.1 6.1.2 6.1.3	Certification body personnel General Management of Competence for personnel involved in the certification process Contract with the personnel	4.1 4.1.1 4.1.2 4.1.3
13.	6.2	Resources for evaluation	4.2
14.	7	Process Requirement	Section 5

15.	7.1	General	5.1
16.	7.2	Application	5.2
17.	7.3	Application review	5.3
18.	7.4	Evaluation	5.4
19.	7.5	Review	5.5
20.	7.6	Certification Decision	5.6
21.	7.7	Certification documentation	5.7
22.	7.8	Directory of certified products	5.8
23.	7.9	Surveillance	5.9
24.	7.10	Changes affecting certification	5.10
25.	7.11	Termination, Reduction, Suspension or Withdrawal of certification	5.11
26.	7.12	Records	5.12
27.	7.13	Complains and appeals	5.13
28.	8	Management system requirements	Section 6
29.	8.1	Options	----
30.	8.2	General management system documentation (Option A)	6.2
31.	8.3	Control of documents (Option A)	6.3
32.	8.4	Control of records (Option A)	6.4
33.	8.5	Management review (Option A)	6.6
34.	8.6	Internal audits (Option A)	6.5
35.	8.7	Corrective actions (Option A)	6.7
36.	8.8	Preventive actions (Option A)	6.7

Annexure-V: Mapping with CCRA Requirements

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"

S. No.	Item	Verdict (Y/N/I)	Evidence
1.	Check that the services of the Certification Body are to be available without undue financial or other conditions. (C.1)	Y	STQC/CC/D02 – Clause2.4.1
2.	Check that the procedures under which the Certification Body operates are to be administered in a non-discriminatory manner. (C.1)	Y	STQC/CC/D02 - Clause 2.4.2,
3.	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)	Y	STQC/CC/D02 –Clause 2.2

S. No.	Item	Verdict (Y/N/I)	Evidence
4.	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.(C.3)	Y Y Y Y	STQC/CC/D02 - Clause 3.1 - Annexure III STQC/CC/D02 – Clause2.3.2 STQC/CC/D01, Master-list of Documents STQC/CC/D02 - Clause 2.1
5.	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	Y	STQC/CC/D02 - Clause3.1 STQC/CC/D17

S. No.	Item	Verdict (Y/N/I)	Evidence
	also provide evidence.]		
6.	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)	Y	STQC/CC/D02 - Clause 4.1 & 4.2
7.	Check that personnel have clear, up-to-date, and documented instructions pertaining to their duties and responsibilities available to them. (C.4)	Y	STQC/CC/D02 - Clause 3.1.3 & 3.1.5 STQC/CC/D12
8.	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,	NO OUTSOURCING	Not Applicable

S. No.	Item	Verdict (Y/N/I)	Evidence
	which can be done by an outside body with the relevant experience and qualifications.]		
9.	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 amendedor superseded without proper authorisation; c) Changes are promulgated insuch way that those who need to know are promptlyinformed and are in a position to take prompt and effective action; d) Superseded documents are removed from use throughout the organisation and itsagencies; e) Those with a direct interest	Y	STQC//CC/D02– Clause 6.3 STQC/CC/P05

S. No.	Item	Verdict (Y/N/I)	Evidence
	in the Scheme are informed of changes. (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.]		
10.	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.]	Y	STQC/CC/D02–Clause 5.12 STQC/CC/P06
11.	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	Y	STQC/CC/P06

S. No.	Item	Verdict (Y/N/I)	Evidence
	traced. (C.6)		
12.	Check that all records are securely and accessibly stored for a period of at least five years. (C.6)	Y	STQC/CC/P06
13.	Check that the Certification Body has the required facilities and 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)	Y	STQC/CC/D03 STQC/CC/D04
14.	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)	Y	STQC/CC/D03, STQC/CC/D04

S. No.	Item	Verdict (Y/N/I)	Evidence
15.	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.]	Y	STQC/CC/D03, STQC/CC/D04, STQC/CC/F16
16.	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)	Y	STQC/CC/D03, STQC/CC/D04, STQC/CC/F16
17.	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)	Y	STQC/CC/D03, STQC/CC/D04 STQC/CC/F16

S. No.	Item	Verdict (Y/N/I)	Evidence
18.	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 as per evaluator basis although this is recommended.]		STQC/CC/D04 STQC/CC/F16
19.	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)	Y	STQC/CC/D02- Clause 2.1.2 STQC/CC/D14 STQC/CC/F15

S. No.	Item	Verdict (Y/N/I)	Evidence
20.	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 atleast:	Y	STQC/CC/D02
	a) A policy statement on the maintenance of quality;	Y	STQC/CC/D02 – Clause 6.1
	b) A brief description of the legal status of the Certification Body;	Y	STQC/CC/D02 – Clause 2.1.1
	c) The names, qualifications and duties of the senior executive and other certification personnel;	Y	STQC/CC/D02 – Clause 3.1 & 4.2
	d) Details of training arrangements for certification personnel;	Y	STQC/CC/P02
	e) An organisation chart showing lines of authority, responsibility and allocation of functions stemming from the senior executive;	Y	STQC/CC/D02 – ANNEX III
	f) Details of procedures for monitoring IT product or Protection Profile evaluations;	Y	STQC/CC/D08, STQC/CC/D09
	g) Details of procedures for preventing the abuse of Common Criteria certificates;	Y	STQC/CC/D02 – 2.1.3 STQC/CC/D13
	h) The identities of any		Not Applicable

S. No.	Item	Verdict (Y/N/I)	Evidence
	contractors and details of the documented procedures for assessing and monitoring their competence; i) Details of any procedures for appeals or conciliation.(C.9)	NO OUTSOURCING Y	 STQC/CC/D02 Clause 5.13 STQC/CC/P07
21.	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)	Y	STQC/CC/D02 – Clause 2.5
22.	Check the application of the procedures to ensure the confidentiality of protected information (C.10)	Y	STQC/CC/P06
23.	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 VPA 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.]	Y	STQC/CC/D02 – Clause 2.5 STQC/CC/F07

S. No.	Item	Verdict (Y/N/I)	Evidence
24.	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]	Y	STQC/CC/D15, STQC/CC/F11
25.	Check that the Certification Body has procedures to deal with disagreements among itself, its associated evaluation facilities, and	Y	STQC/CC/P07

S. No.	Item	Verdict (Y/N/I)	Evidence
	their clients. (C.12)		
26.	Check that the Certification Body undertakes management reviews of its operations to ensure that it continues to share the CCRA objectives. (C.13)	Y	STQC/CC/P04
27.	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)	Y	STQC/CC/D02 – Clause 2.1.3 STQC/CC/D13
28.	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)	Y	STQC/CC/D02 – Clause 5.11