

IC3S

Requirements for Testing Laboratories (STQC/CC/D04) Issue :06



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

| | | |
|---|---|-------------------|
|  | <h1>Indian CC Certification Scheme</h1> | |
| | D04– Requirements for Testing Laboratories | Issue : 06 |
| | | Date : 29-05-2020 |
| | | Page : 2 of 24 |

Table of Contents

| | | |
|------|--|-------------------------------------|
| 0.1 | Foreword | 4 |
| 0.2 | Approval and Issue | 5 |
| 0.3 | Amendment Record | 6 |
| 1.0 | Introduction | 7 |
| 1.1 | Background | 7 |
| 1.2 | Purpose..... | 7 |
| 2.0 | Reference | 7 |
| 3.0 | Evaluation Activity of CCTL..... | 8 |
| 3.1 | Scope | 8 |
| 3.2 | Security Services under Test..... | 9 |
| 3.3 | Security Features under Test | 9 |
| 3.4 | Test Techniques | 9 |
| 3.5 | Testing Approach | 10 |
| 3.6 | Proficiency Testing | Error! Bookmark not defined. |
| 4.0 | Management Requirements for approval of CCTL | 11 |
| 4.1 | Organization..... | 11 |
| 4.2 | Management system..... | 12 |
| 4.3 | Document control | 12 |
| 4.4 | Review of requests, tenders and contracts | 12 |
| 4.5 | Subcontracting of Evaluation activities | 12 |
| 4.6 | Service to the customer | 12 |
| 4.7 | Complaints..... | 12 |
| 4.8 | Control of nonconforming testing and/or calibration work | 12 |
| 4.9 | Improvement | 12 |
| 4.10 | Corrective action | 13 |
| 4.11 | Preventive action..... | 13 |
| 4.12 | Control of records | 13 |

| | | |
|---|---|-------------------|
|  | Indian CC Certification Scheme | |
| | D04– Requirements for Testing Laboratories | Issue : 06 |
| | | Date : 29-05-2020 |
| | Page : 3 of 24 | |

| | | |
|-------|---|----|
| 4.13 | Internal audits | 13 |
| 4.14 | Management reviews..... | 14 |
| 5.0 | Technical Requirements for approval of CCTL..... | 15 |
| 5.1 | General..... | 15 |
| 5.2 | Personnel | 15 |
| 5.3 | Accommodation and environmental conditions | 15 |
| 5.4 | Test and calibration methods and method validation..... | 16 |
| 5.5 | Equipment | 17 |
| 5.6 | Measurement traceability | 18 |
| 5.7 | Sampling | 18 |
| 5.8 | Handling of test and calibration items | 18 |
| 5.9 | Assuring the quality of test and calibration results..... | 18 |
| 5.10 | Reporting the results..... | 18 |
| 6.0 | Scheme Specific Requirements..... | 19 |
| 6.1 | Specific Requirements | 19 |
| 6.1.1 | Conflict of interest requirements | 19 |
| 6.1.2 | Facility requirements..... | 20 |
| 6.1.3 | Personnel requirements..... | 21 |
| 6.1.4 | Evaluation operational requirements | 21 |

| | | |
|---|---|-------------------|
|  STQC ॥ गुणोत्कर्षं समृद्धिः ॥ | <h1>Indian CC Certification Scheme</h1> | |
| | <h2>D04– Requirements for Testing Laboratories</h2> | Issue : 06 |
| | | Date : 29-05-2020 |
| | Page : 4 of 24 | |

0.1 Foreword

This document defines the requirements relating to Organizational and Technical functions of Common Criteria Testing Laboratories (CCTL), in addition to requirements of ISO/IEC 17025, for being approved and continuing with the approval under the Indian Common Criteria Certification Scheme(IC3S).

| | | |
|--|---|-------------------|
|  गुणोत्कर्षं समृद्धिः | <h1>Indian CC Certification Scheme</h1> | |
| | D04– Requirements for Testing Laboratories | Issue : 06 |
| | | Date : 29-05-2020 |
| | Page : 5 of 24 | |

0.2 Approval and Issue

This document is the property of Indian Common Criteria Certification Scheme (IC3S) and should not be reproduced in part or full without the written consent.

Reviewed by : Management Representative

Approved by : Head, CC Scheme

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.

| | | |
|---|---|-------------------|
|  | <h1>Indian CC Certification Scheme</h1> | |
| | D04– Requirements for Testing Laboratories | Issue : 06 |
| | | Date : 29-05-2020 |
| | | Page : 7 of 24 |

1.0 Introduction

1.1 Background

Indian Common Criteria Certification Scheme (IC3S) is operated by STQC Directorate, Ministry of Electronics and Information Technology (MeitY), Govt. of India. Under the IC3S scheme, the Evaluation Laboratories or Common Criteria Test laboratories (henceforth will be referred as CCTLs) perform evaluations of Information Technology (henceforth will be referred as IT) security products against the requirements of ISO 15408 or Common Criteria Standards. The Certification Body (CB) of IC3S is responsible for approving the evaluation laboratories as authorized CCTL. This guideline document explains the technical requirements of an approved CCTL operating under IC3S. The basis of this document is ISO/IEC 17025: General Requirements for the Competence of Testing and Calibration Laboratories. Any facility or laboratory operating within Indian Territory that performs evaluation of IT security products may apply for approval under IC3S. The approval process defined in the document, Requirements for Testing Laboratories for Enlistment and Operation under IC3S (STQC/CC/D03) considers the requirements detailed in this document.

1.2 Purpose

This document is intended for information and use by accreditation team or approvers of CCTLs, staff of the approved CCTLs, those facilities seeking approval under IC3S and other stake holders of Common Criteria or ISO/IEC 15408 evaluation activities.

The purpose of this document is to amplify where appropriate, generic, technical and organization criteria as stated in ISO/IEC 17025: General Requirements for the Competence of Testing and Calibration Laboratories, for approval of the facilities or laboratories that could perform evaluation of IT security products as per the requirements of ISO/IEC 15408 or Common Criteria Standard under IC3S.

2.0 Reference

STQC/CC/D02 : Quality Manual of the Certification Body

| | | |
|---|---|-------------------|
|  | <h1>Indian CC Certification Scheme</h1> | |
| | D04– Requirements for Testing Laboratories | Issue : 06 |
| | | Date : 29-05-2020 |
| | | Page : 8 of 24 |

- STQC/CC/D03 : Accreditation Process for Enlistment and Operation of labs under IC3S.
- ISO/IEC 17025 : General Requirements for the Competence of Testing and Calibration Laboratories.
- ISO/IEC 15408 : Evaluation Criteria for IT Security:
- Part 1 : Introduction and general model;
 - Part 2 : Security functional requirements; and
 - Part 3 : Security assurance requirements
- ISO/IEC 18045 : Information technology -- Security techniques -- Methodology for IT security evaluation
- CC Part 1 : Common Criteria - Introduction and general model.
- CC Part 2 : Security functional requirements
- CC Part 3 : Security assurance requirements
- CEM : Common Methodology for Information Technology Security Evaluation

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

3.0 Evaluation Activity of CCTL

3.1 Scope

The evaluation activities of CCTL shall include tests such as Security functional test, penetration tests etc. which may require a great deal of interpretation, such as the implementation of robustness of the security functions of IT products.

| | | |
|---|---|-------------------|
|  | <h1>Indian CC Certification Scheme</h1> | |
| | D04– Requirements for Testing Laboratories | Issue : 06 |
| | | Date : 29-05-2020 |
| | Page : 9 of 24 | |

3.2 Security Services under Test

CCTL involves the analysis of security features implemented within a software/hardware/ ITS product which can provide the following security services, as applicable:

- Confidentiality of information
- Integrity of information
- Availability
- Accountability

3.3 Security Features under Test

Specific security features that can be tested for may include but are not limited to the following:

- Identification and authentication
- Security audit (audit trail generation and secure storage, analysis of security relevant events);
- Implementation of Cryptographic services (cryptographic operations, cryptographic key management);
- Secure transport of information (implementation and enforcement of access control and/or information flow rules/policies);
- Management of security functions, security relevant data and security management role
- Protection of security functions
- Resource utilization (fault tolerance, priority of service, resource allocation), Fail-safe
- Self-test and Physical protection (tamper detection/prevention)

3.4 Test Techniques

Techniques to be used for evaluation of security features of the IT security products to include but not limited to the following:

- Analysis of documentation of security functional and assurance requirements
- Analysis of documentation on product functional specification, architecture, design and implementation details

| | | |
|---|---|-------------------|
|  | <h1>Indian CC Certification Scheme</h1> | |
| | D04– Requirements for Testing Laboratories | Issue : 06 |
| | | Date : 29-05-2020 |
| | | Page : 10 of 24 |

- Testing of the product with expected behavior of the product (Known answer test)
- Vulnerability search and analysis for the type of product and verify that the product is able to resist attacks with a definite attack potential(pertaining to the EAL) intended to exploit the identified vulnerabilities.
 - The Evaluators must consider public domain vulnerability information and various evaluation evidences like Functional Specification document, Design document, Guidance Document, delivery procedure etc. relevant to the TOE. The activity shall be performed as per documented procedure
 - Evaluators shall also ensure through adequate testing that new vulnerabilities are not added as a result of resolving a function or mitigating an identified vulnerability
- Assessment of development environment through analysis of process documentation related to the development of the product and site visit.
- Analysis of tests conducted by the developer for coverage and depth
- Analysis of configuration management system used for development of the product
- Analysis of product delivery procedure
- Analysis of product guidance documents to be used by users and administrators

3.5 Testing Approach

The testing approach to be followed by CCTL should clearly address the following:

- a) Complete coverage of the security features of the product under evaluation
- b) Test plans clearly identifying the features to be tested, equipment and resources to be used, preprocessing and post processing necessary for the test etc.
- c) Detailed test procedure
- d) Alternative Test approach, if any, with the approval of CB
- e) Expected result

| | | |
|---|---|-------------------|
|  | <h1>Indian CC Certification Scheme</h1> | |
| | D04– Requirements for Testing Laboratories | Issue : 06 |
| | | Date : 29-05-2020 |
| | Page : 11 of 24 | |

f) Actual result

4.0 Management Requirements for approval of CCTL

The laboratory shall have a Management System which meets the requirements of ISO/IEC 17025. Additionally, the laboratory shall meet the following Management and Technical requirements.

4.1 Organization

The CCTL shall establish and maintain policies and procedures to ensure impartiality and integrity while conducting Common Criteria evaluations. The laboratory policies and procedures shall ensure that:

- a) CCTL staff members cannot both develop and evaluate the same Protection Profile, Security Target, or IT product, and
- b) CCTL staff members cannot provide consulting services for and then participate in the evaluation of the same Protection Profile, Security Target, or IT product.

The CCTL shall have physical and electronic controls for maintaining separation (both physical and electronic) among the stakeholders (e.g. evaluators, product developers, system integrators etc.) to avoid undue influence on the evaluation outcome.

The management system shall include policies and procedures to ensure the protection of proprietary information. This protection shall specify how proprietary information will be protected from persons outside the CCTL, from visitors to the laboratory, from laboratory personnel without a need to know, and from other unauthorized persons.

| | | |
|---|---|-------------------|
|  | <h1>Indian CC Certification Scheme</h1> | |
| | D04– Requirements for Testing Laboratories | Issue : 06 |
| | | Date : 29-05-2020 |
| | Page : 12 of 24 | |

4.2 Management system

The management system requirements are designed to promote laboratory practices that ensure technical accuracy and integrity of the security evaluation and adherence to quality assurance practices appropriate to Common Criteria Testing. The laboratory shall maintain a management system that fully documents the laboratory's policies, practices, and the specific steps taken to ensure the quality of the IT security evaluations.

The reference documents, standards, and publications listed in section 2 shall be available for use by laboratory staff developing and maintaining the management system and conducting evaluations.

Records shall be kept of all management system activities.

4.3 Document control

There are no requirements additional to those specified in ISO/IEC 17025.

4.4 Review of requests, tenders and contracts

The procedures for review of contracts shall include procedures to ensure that the laboratory has adequate evaluators, technical staffs and resources to meet its evaluation schedule and complete evaluations in a timely manner.

4.5 Subcontracting of Evaluation activities

Subcontracting of evaluation activities shall not be allowed.

4.6 Service to the customer

There are no requirements additional to those specified in ISO/IEC 17025.

4.7 Complaints

There are no requirements additional to those specified in ISO/IEC 17025.

4.8 Control of nonconforming testing and/or calibration work

There are no requirements additional to those specified in ISO/IEC 17025.

4.9 Improvement

There are no requirements additional to those specified in ISO/IEC 17025.

| | | |
|---|---|-------------------|
|  | <h1>Indian CC Certification Scheme</h1> | |
| | D04– Requirements for Testing Laboratories | Issue : 06 |
| | | Date : 29-05-2020 |
| | | Page : 13 of 24 |

4.10 Corrective action

There are no requirements additional to those specified in ISO/IEC 17025.

4.11 Preventive action

There are no requirements additional to those specified in ISO/IEC 17025.

4.12 Control of records

The CCTL shall maintain a functional record-keeping system that is used to track each security evaluation Records shall be easily accessible and contain complete information for each evaluation. Required records of evaluation activities shall be traceable to Common Criteria evaluator actions and Common Evaluation Methodology work units or ISO 18045 work units. Computer-based records shall contain entries indicating the date created and the individual(s) who performed the work, along with any other information required by the management system. Records in hard copies shall be dated and signed. All records shall be maintained in accordance with CCTL policies and procedures and in a manner that ensures record integrity. There shall be appropriate back-ups and archives.

There must be enough evaluation evidence in the records so that an independent body, including CB, can determine what evaluation work was actually performed for each work unit and can harmonize with the verdict. Records include evaluator worksheets, records relating to the TOE, test data/test screen shots and records received from the developer.

CCTL records shall be retained for a period of at least five years. Beyond this requirement, laboratory records shall be maintained, released, or destroyed in accordance with the laboratory's proprietary information policy and contractual agreements with customers.

4.13 Internal audits

The internal audit shall cover the laboratory management system and the application of the management system to all laboratory activities. The audit shall cover compliance with ISO 17025 requirements along with scheme specific requirements. Audits shall cover all aspects of the evaluation activities, including the evaluation work performed.

| | | |
|---|---|-------------------|
|  | <h1>Indian CC Certification Scheme</h1> | |
| | D04– Requirements for Testing Laboratories | Issue : 06 |
| | | Date : 29-05-2020 |
| | Page : 14 of 24 | |

The CCTL laboratory person should not audit his own area of work. In the case where only one member of the laboratory staff is competent to conduct a specific aspect of a test method, and performing an audit of work in this area would result in that person auditing his or her own work, then audits may be conducted by another staff member. The audit shall cover the evaluation methodology for that test method and shall include a review of documented procedures and instructions, adherence to procedures and instructions, and review of previous audit reports. External experts may also be used in these situations.

The internal audit reports shall be available for review during on-site assessments by CB.

The laboratory shall perform at least one complete internal audit prior to the first full on-site assessment.

4.14 Management reviews

CCTL shall comply the requirements of ISO/IEC 17025 in this regard. The records of the management review shall be made available to CB or its appointed team during site visit. The laboratory shall perform at least one management review prior to on-site assessment.

| | | |
|---|---|-------------------|
|  | <h1>Indian CC Certification Scheme</h1> | |
| | D04– Requirements for Testing Laboratories | Issue : 06 |
| | | Date : 29-05-2020 |
| | | Page : 15 of 24 |

5.0 Technical Requirements for approval of CCTL

5.1 General

The CCTL shall have a quality manual describing the details process or procedure addressing the technical requirements of ISO/IEC 17025 and scheme specific requirements as defined under section 6.0.

5.2 Personnel

The CCTL shall have at least two technical staff members with appropriate educational background (preferably, a university graduate degree in Science/Computerscience/electronics or engineering and professional Certification in specific area of technology related to the product being evaluated by the CCTL) and relevant experience in development/testing of IT security product.

The laboratory shall maintain position descriptions, training records and resumes for responsible supervisory personnel and laboratory staff members who have an effect on the outcome of security evaluations.

The laboratory management system shall document the policies and procedures (training program) governing the competence to conduct a Common Criteria evaluation.

The laboratory shall also designate one responsible person as quality manager who has overall responsibility for the management system, the quality system, and maintenance of the management system documents.

The laboratory shall notify CBany change in key personnel. When key laboratory staff is added, the notification of changes shall include a current resume for each new staff member.

5.3 Accommodation and environmental conditions

The laboratory shall have adequate facilities to conduct IT security evaluations. This includes facilities for security evaluation, staff training, record keeping, document storage, and software storage.

A protection system shall be in place to safeguard customer proprietary hardware, software, test data, electronic and paper records, and other materials. This system shall protect the proprietary materials and information from personnel outside the

| | | |
|---|---|-------------------|
|  | <h1>Indian CC Certification Scheme</h1> | |
| | D04– Requirements for Testing Laboratories | Issue : 06 |
| | | Date : 29-05-2020 |
| | Page : 16 of 24 | |

laboratory, visitors to the laboratory, laboratory personnel without a need to know, and other unauthorized persons. Laboratories shall have systems (e.g., firewall, intrusion detection) in place to protect internal systems from untrusted external entities.

CCTL shall have regularly updated protection for all systems against viruses and other malware. The laboratory shall have an effective backup system to ensure that data and records can be restored in the event of their loss.

CCTL networks used to conduct ATE and AVA evaluation activities shall be completely isolated.

If CCTL is conducting multiple simultaneous evaluations, it shall maintain a system of separation between the products of different customers and evaluations. This includes the product under evaluation, the test platform, peripherals, documentation, electronic media, manuals, and records.

When testing is performed at the developer's premises or other location outside CCTL, all the requirements of this document pertaining to equipment, accommodation and environment shall apply.

The soft copies of the evaluation evidences and objects shall be encrypted while transferring those over Internet (for communication with the developer and/or validator) and encrypted communication channel shall be used for this purpose.

5.4 Test and calibration methods and method validation

The test methods of ISO/IEC 17025 are analogous to evaluation methodology using the Common Criteria (CC), the Common Evaluation Methodology (CEM), and additional laboratory-developed methodology. The version of the CC and CEM to be used in each evaluation shall be established in consultation with CB and the sponsor.

For the purposes of achieving product validation through the Common Criteria or ISO 15408 Scheme, laboratories may be required to comply with both international interpretations and CB specified guidance. CB may issue guidance or interpretations to supplement the evaluation assurance criteria or methodology provided in the Common Criteria and Common Evaluation Methodology. The

| | | |
|---|---|-------------------|
|  | <h1>Indian CC Certification Scheme</h1> | |
| | D04– Requirements for Testing Laboratories | Issue : 06 |
| | | Date : 29-05-2020 |
| | Page : 17 of 24 | |

laboratory shall comply with the guidance or interpretations within the timeframe specified by CB.

CCTL shall have documented procedures for conducting security evaluations using the Common Criteria and Common Evaluation Methodology, and for complying with guidance or interpretations. CCTL shall ensure that these procedures are followed.

Security evaluations may be conducted at the developer site, the laboratory or another location that is mutually agreed to by the CCTL, the sponsor, and CB. When evaluation activities are conducted outside the laboratory, the laboratory shall have additional procedures to ensure the integrity of all tests and recorded results. These procedures shall also ensure that the same requirements that apply to the laboratory and its facility are maintained at the non-laboratory site.

When exceptions to the evaluation methodology are deemed necessary for technical reasons, CB designated validator of the project shall be consulted to ensure that the new methodology continues to meet all requirements and policies, the customer shall be informed, and details of these exceptions shall be described in the evaluation report.

5.5 Equipment

CCTL shall maintain adequate systems to support IT security evaluations in keeping with the tests for which it is seeking accreditation. The laboratory shall have an electronic repository with version control capability and shall have capability to generate electronic reports.

CCTL shall document and maintain records on all test equipment or test suites used during Common Criteria testing. The laboratory shall be responsible for configuration and operation of all equipment within its control.

Computer systems and other platforms used during Common Criteria testing shall be under configuration control. CCTL shall have procedures to ensure that any equipment (hardware and software) used for testing is in a known state prior to use for testing.

| | | |
|---|---|-------------------|
|  | <h1>Indian CC Certification Scheme</h1> | |
| | D04– Requirements for Testing Laboratories | Issue : 06 |
| | | Date : 29-05-2020 |
| | Page : 18 of 24 | |

5.6 Measurement traceability

For Common Criteria Testing, “Traceability” is interpreted to mean that security evaluation activities are traceable to the underlying Common Criteria requirements and work units in the Common Evaluation Methodology or ISO/IEC 18045. This means that test tools and evaluation methodology demonstrate that the tests they conduct and the test assertions they make are traceable to specific criteria and methodology. This is necessary to ensure that test results constitute credible evidence of compliance with the CC or IS/IEC 15408 and CEM or ISO/IEC 18045.

5.7 Sampling

At present sampling is not applicable.

5.8 Handling of test and calibration items

CCTL shall protect products under evaluation and calibrated tools from modification, unauthorized access, and use. The laboratory shall maintain separation between the items from different evaluations, to include the product under evaluation, its platform, peripherals, and documentation.

When the product under evaluation includes software components, CCTL shall ensure that configuration management mechanisms are in place to prevent inadvertent modifications to the software components during the evaluation process.

CCTL shall have procedures to ensure proper retention, disposal or return of software and hardware after the completion of the evaluation.

5.9 Assuring the quality of test and calibration results

CCTL shall have procedures for conducting final review of evaluation results, the ETR, and the laboratory records of the evaluation prior to their submission to the customer and/or CB.

5.10 Reporting the results

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. Evaluation reports shall provide all

| | | |
|---|---|-------------------|
|  | <h1>Indian CC Certification Scheme</h1> | |
| | D04– Requirements for Testing Laboratories | Issue : 06 |
| | | Date : 29-05-2020 |
| | Page : 19 of 24 | |

necessary information to permit the same or another laboratory to reproduce the evaluation and obtain comparable results.

Evaluation reports created for submission to CB shall meet the requirements of the Common Criteria Scheme. The evaluation report shall contain sufficient information for the exact test conditions and results to be reproduced at a later time if a re-examination or retest is necessary.

Evaluation reports shall be submitted to CB or its designated validator of the project. The form and method of submission, if specified by CB, shall be followed.

6.0 Scheme Specific Requirements

This section discusses in detail the scheme specific requirements that a prospective CCTL must meet. These requirements are subdivided into the following categories:

6.1 Specific Requirements

- Conflict of interest requirements which are concerned with the degree of organizational separation within the prospective CCTL, to ensure that all CC evaluation work is performed in an objective manner, without undue influence from within the facility.
- Facility requirements which are concerned with a CCTL's physical and IT infrastructure, and overall security;
- Personnel requirements which are concerned with the technical competence of each CCTL staff member.
- Evaluation operational requirements which are concerned with IC3S scheme related work focusing the requirements of Common Evaluation Methodology (CEM) or ISO 18045

6.1.1 Conflict of interest requirements

If the testing laboratory seeking for approval from CB is controlled by a parent company, then the laboratory must demonstrate that there is sufficient separation

| | | |
|---|---|-------------------|
|  | <h1>Indian CC Certification Scheme</h1> | |
| | D04– Requirements for Testing Laboratories | Issue : 06 |
| | | Date : 29-05-2020 |
| | Page : 20 of 24 | |

of control and influence on the outcome of CC evaluation activities. The laboratory shall demonstrate with objective evidences that:

- The parent company cannot exert undue influence on the outcome of the CC evaluation activities
- Proprietary evaluation information cannot be inappropriately accessed by the parent company.

The CCTL must have appropriate procedure in place to ensure that there is no conflict of interest between personnel offering their consultancy services to the developer or sponsor (on the aspect of CC evaluation of an IT security product) and the personnel actually performing evaluation of that particular IT security product.

The laboratory must have procedures in place to ensure that management cannot exert undue influence on the outcome of CC evaluation activities.

6.1.2 Facility requirements

The following scheme-specific requirements are imposed by CB on approved CCTLs:

- I. Must reside within India and be a legal entity, duly organized and incorporated, validly existing, and in good standing under the laws of the state where the laboratory intends to do business.
- II. The laboratory must retain their evaluation and testing facilities permanently in India and have communication facilities like telephone (landline), Fax, e-Mail ID
- III. The laboratory must have sufficient office space and equipment space available. Also space for at least one member of the Certification Body to work in the performance of evaluation technical oversight, when required.
- IV. The evaluation facility should be both physically and logically isolated from the rest of the organization with proper physical and logical security mechanism at the boundaries to ensure confidentiality of evaluation activities and their outcome.
- V. The laboratory must have or be able to provide with sufficient IT infrastructure
 - a) To support general documentation and for producing reports.
 - b) Tools to protect documents from tampering

| | | |
|---|---|-------------------|
|  | <h1>Indian CC Certification Scheme</h1> | |
| | D04– Requirements for Testing Laboratories | Issue : 06 |
| | | Date : 29-05-2020 |
| | Page : 21 of 24 | |

- c) To maintain confidentiality of the reports
 - d) Access to Internet
 - e) To exchange evaluation objects and evaluation outcome securely with the developer/sponsor or validator/Certification body.
- VI. The laboratory should have proper facility to protect the evaluation records and objectives, if those are in the form of hardcopies.
- VII. The laboratory must be equipped with necessary equipment, tools etc. relevant to the area of technology for which approval from CB is sought.

4.1.1 Personnel requirements

The potential CCTL should have a minimum of two personnel in their employee role who have been empanelled or proposed to be empanelled as CC evaluators after meeting the following requirements:

- Knowledge and experience in IT Security
- Knowledge of the CC or ISO 15408 and CEM or ISO 18045

Proposed CC evaluators are those individuals of the evaluation laboratory who has sufficient, demonstrable knowledge and experience in the area of IT security testing/assessment and whose knowledge on Common Criteria (ISO 15408) and Common Evaluation Methodology (ISO 18045) are yet to be evaluated by the certification body.

4.1.2 Evaluation operational requirements

The evaluation laboratory must comply with the evaluation operational requirements as documented below:

- I. Scheme Related Work: The CCTL must keep the CB informed of all Scheme related work that is being performed.
- II. Registration for evaluation and Certification Services: The evaluation and certification projects shall only be registered through CB. In case the developer/sponsor contacts the CCTL in this regard, CCTL shall direct them to CB.
- III. Evaluation Tasks: The CCTL must partition its work into discrete tasks. For the purposes of planning and reporting, a task corresponds to the

| | | |
|---|---|-------------------|
|  | <h1>Indian CC Certification Scheme</h1> | |
| | D04– Requirements for Testing Laboratories | Issue : 06 |
| | | Date : 29-05-2020 |
| | Page : 22 of 24 | |

work performed by a CCTL for the evaluation of a single TOE. A task must be uniquely identified throughout its life-time. The identification shall be such that the TOE and related items cannot be confused physically or when referenced in records or other documents.

- IV. Supply of Documentation to the CB: All documentation supplied by the CCTL to CB must be in encrypted softcopy format, either on suitable removable media or through secure repository or through secure email.
- V. Task Initiation: The CCTL shall communicate CB when it is ready to perform an evaluation task.
- VI. Task Confidentiality: Task information must be handled so that its confidentiality is maintained and the same is agreed upon through an agreement with the developer or sponsor. CCTL must ensure signing of confidentiality agreement with evaluators.
- VII. Evaluation Work Plan (EWP): CCTL must agree their Evaluation Work Plan at the Task Startup Meeting to communicate task specific details of the evaluation process to CB.
- VIII. Task Startup Meeting: The CCTL must attend a Task Startup Meeting if required. If a Task Startup Meeting is not held then the CCTL, the Sponsor and the CB must address by other informal means all of the relevant issues that would otherwise be covered in a Task Startup Meeting.
- IX. Deliverables List: The CCTL must ensure that the Sponsor/developer has contractually agreed to supply deliverables appropriate to the scope of evaluation and target assurance level.
- X. Security Target Review: Following the Task Startup Meeting, the Evaluators must:
 - a. carry out the formal evaluation of the Security Target according to the appropriate criteria and methodology, and
 - b. ensure that the Security Target defines a TOE which corresponds to the scope of evaluation agreed at the Task Startup Meeting.
- XI. Evaluation Process: In addition to analysis of product and development process documentations, the evaluators shall conduct independent testing of TOE and also consider public domain vulnerability information

| | | |
|---|--|-------------------|
|  | <h2 style="color: blue;">Indian CC Certification Scheme</h2> | |
| | D04– Requirements for Testing Laboratories | Issue : 06 |
| | | Date : 29-05-2020 |
| | Page : 23 of 24 | |

and various evaluation evidences like Functional Specification document, Design document, Guidance Document, delivery procedure etc. for vulnerability assessment of the TOE.

- XII. Evaluation Progress Reviews: CB shall review all ongoing evaluation projects every six months. Decisions on problems encountered, if any, shall be taken in the reviews.
- XIII. Task Records: For each task, the Evaluators must ensure that a systematic record of all information is maintained in accordance with the CCTL's Quality Manual.
- XIV. Observation Reports: Evaluators must raise ORs to draw attention of the developer or sponsor to deficiencies of the evaluation objects with respect to the requirements of ISO 15408 or CC Standards and other problems, as and when they are discovered, during an evaluation and communicate the same to the developer/ sponsor securely.
- XV. Evaluation Work Sheets: Evaluators shall document their evaluation results in the form of work sheets addressing the requirements of CEM. The same shall be presented for validation.
- XVI. Evaluation Technical Report: The CCTL must produce a final ETR and supply a copy to CB. The ETR must precisely identify the evaluated TOE and address all the requirements of CEM or ISO 18045. The ETR must include a deliverables list. The Evaluators must report work performed and the detailed results in the ETR, as required by CEM, giving sufficient justifications for verdicts and conclusions.
- XVII. Test records: Evaluators must ensure that scripts for penetration tests and additional implementation tests are recorded in sufficient detail to allow repeatability and reproducibility. When a tool is used to assess one or more test items this must be recorded in sufficient detail to allow repeatability or reproducibility.
- XVIII. Closure: When the CCTL has completed the evaluation work and the Certification Report has been agreed and issued, the CCTL can close down the project. In the closure process, CCTL shall archive or dispose of all material supplied for the evaluation as defined by CB and decided in initial meeting with the developer/sponsor.

| | | |
|---|---|-------------------|
|  STQC ॥ गुणोत्कर्षं समृद्धिः ॥ | <h2>Indian CC Certification Scheme</h2> | |
| | D04– Requirements for Testing Laboratories | Issue : 06 |
| | | Date : 29-05-2020 |
| | Page : 24 of 24 | |

Adequate records shall be retained by both the CCTL to ensure the reproducibility and repeatability of the task.