CCC SP-101-2

Singapore Common Criteria Scheme

BY CYBER SECURITY AGENCY OF SINGAPORE

Publication No. 2

Requirements for Approving Common Criteria Test Laboratory (CCTL)

June 2024
Version 8.0

Amendment Record

Version	Date	Author	Changes
1-3	August, 2009	Infocomm Development Authority of Singapore	Release
4.0	October, 2017	Cyber Security Agency of Singapore	Alignment to CSA processes.
5.0	June, 2018	Cyber Security Agency of Singapore	Minor editorial revisions
6.0	January 2019	Cyber Security Agency of Singapore	Minor editorial revisions
7.0	April 2020	Cyber Security Agency of Singapore	Minor editorial revisions
7.1	May 2024	Cyber Security Agency of Singapore	Minor editorial revisions
8.0	June 2024	Cyber Security Agency of Singapore	Transition to CC:2022

Contents

1 INTRODUCTION

1.0.1 The Cyber Security Agency Evaluation Authority (CSA) is responsible for approving Common Criteria Testing Laboratories (CCTL) to perform evaluation of IT products under the Singapore Common Criteria Scheme (SCCS). CSA is also responsible for monitoring all the evaluations of IT products performed under the SCCS.

1.0.2 Any testing laboratory that conducts, or intends to conduct, the business of IT security testing and evaluation under the SCCS, must apply to CSA for approval to be a CCTL.

1.1 Purpose and scope

1.1.1 This document defines the process to be followed and the conditions and requirements to be fulfilled by the applicant seeking to be appointed as a CCTL.

1.1.2 The intended applicants should primarily be testing laboratories interested in joining the SCCS. The approval of the testing laboratory as a CCTL would provide interested laboratory customers with the assurance that the testing laboratory is approved and has met the stringent security requirements imposed by CSA under the SCCS.

1.1.3 For the purposes of this document, any reference to the term “CCTL” shall include a reference to a holder of a provisional approval (under 5.2) or approval (under 5.3) granted by the CSA.

2 ELIGIBILITY CRITERIA AND OBLIGATIONS FOR PROVISIONAL APPROVED AND APPROVED CCTL

2.1 General Requirements

2.1.1 The evaluation laboratory shall be accredited by the Singapore Accreditation Council (SAC) [1] or by other recognised Accreditation Bodies in accordance with the ISO/IEC 17025 for testing laboratories in the domain of IT security according to the Common Criteria for IT security evaluation (CC). The recognised Accreditation Body shall be a member of the International Accreditation Forum (IAF, http://www.iaf.nu/) and of the International Laboratory Accreditation Cooperation (ILAC, http://www.ilac.org/).

2.1.2 The evaluation laboratory shall have an appropriate security policy, preferably conforming to ISO/IEC 27001 and shall be able to meet the

[1] The SAC is the National Accreditation Body for the independent accreditation of conformity assessment bodies in Singapore. More information regarding SAC is available at www.sac-accreditation.gov.sg.

security requirements for handling protected information relating to the evaluation of IT products. For guidance on implementing information security controls, the evaluation laboratory may refer to ISO/IEC 27002.

2.1.3 It is the responsibility of the evaluation laboratory to carry out its evaluation activities in such a way as to meet the requirements of this document and to satisfy the needs of the customer.

2.1.4 The evaluation laboratory shall demonstrate to CSA that it is able to

a) perform IT security evaluations up to Evaluation Assurance Level 4 augmented with AVA_VAN.5 and ALC_FLR.2 defined in the CC Part 3;

b) apply the CC and Common Evaluation Methodology (CEM) correctly and consistently; and

c) operate in accordance with the SCCS policies and procedures.

2.1.5 The evaluation laboratory, or the organisation of which it is part of, should preferably be a Singapore registered entity that can be held legally responsible under the Singapore laws. The evaluation laboratory shall be ISO/IEC 17025 accredited as stated in 2.1.1 prior to release of any evaluation technical report under the SCCS.

2.1.6 Nonetheless, it is recognised that setting up of a fully equipped evaluation laboratory and recruiting the qualified evaluators require significant investment and are non-trivial. To facilitate the establishment, an existing CCTL approved by another CCRA scheme, operating outside of Singapore, can apply to CSA for approval as a remote CCTL under the SCCS on the following conditions:

a) The CCTL must be a non-governmental legal entity, be duly organized and incorporated and in good standing under the laws of the nation/state where the CCTL is operating from;

b) The CCTL must have technical competency in specific field of IT security evaluation which has been confirmed by another CCRA scheme;

c) The CCTL must be assessed by CSA to ensure that the CCTL complies with the SCCS;

d) The CCTL must comply with all other requirements and conditions stated in the SCCS Publications and IT 001 [3] published by the SAC (www.sac-accreditation.gov.sg)

The SCCS is no longer accepting new applications for remote CCTLs. Any existing remote approval awarded to a CCTL by CSA is valid for two (2) years, subject to CSA's approval being sought for subsequent

extension. CSA reserves the right to revoke the remote approval at any time, if the said CCTL loses its approval under another CCRA scheme or fails to comply with the requirements under the SCCS.

2.2 Impartiality

2.2.1 If the CCTL is part of an organisation that performs activities other than IT security evaluation (e.g. consultation to product developer), the CCTL shall identify actual and potential conflicts of interest and ensure clear separation of control to ensure that there is no undue influence on the evaluation activities.

2.2.2 The CCTL must be an independent evaluation laboratory. It should be free of any undue commercial, financial and other interest of the product that it would be evaluating.

2.2.3 For every project carried out under the SCCS, the CCTL shall declare in the Certificate Application Form (CAF), and if required, prove to CSA that its staff members are free from any undue commercial, financial and other pressures which may influence their technical judgments and affect the outcome of the evaluation.

2.2.4 The CCTL is allowed to provide both consultancy and evaluation services for the same TOE under the SCCS if the CCTL is able to demonstrate its conformance to 2.2.1 and 2.4 with clear role and logical separation procedures in place as well as appointing qualified evaluators and qualified consultants for the project.

2.2.5 CSA is entitled to revoke a CC certificate issued by the SCCS under the conditions described in 6.1 of SCCS Publication #3.

2.3 Quality System

2.3.1 The CCTL shall have and comply with a quality system that conforms to ISO/IEC 17025 for its scope of evaluation activities. This quality system shall be documented in a quality manual, which shall define the CCTL's policies and objectives, roles and responsibilities for managerial and technical staff members and procedures for control of documents and records.

2.3.2 The CCTL shall appoint an ISO/IEC 17025 approved signatory who shall be responsible for making decisions and signing off the test plans, results of the evaluation tasks and ensuring the correctness, consistency and completeness of the evaluation reports. The approved signatory shall be considered one of the staff members and shall be subjected to the same requirements in the following section.

2.4 Staff Members

2.4.1 The CCTL shall have managerial and technical staff members with the authority, qualifications and resources to carry out specific evaluation activities and to identify occurrences of departures from the quality system or from procedures for performing the evaluation activities. At the very minimum, the CCTL shall have two (2) staff members covering the key personnel duties of the following posts: technical manager, business manager, quality manager, security manager and evaluator, with the exception that the roles of quality manager and technical manager cannot be performed by the same staff member.

2.4.2 The CCTL shall be responsible for ensuring that all staff members who perform specific evaluation activities have the relevant IT security qualifications, training and experience, knowledge of CC, and demonstrated skills. At least one (1) principal staff member (inclusive of the approved signatory) shall have practical experience in IT security evaluation and testing to the CC standards.

2.4.3 The CCTL shall have a policy and procedure to identify and provide for the IT security and CC training needs of staff members. Appropriate supervision must be provided to any CCTL staff members who are undergoing CC training.

2.4.4 The CCTL shall maintain accurate records of the current job descriptions for managerial and technical staff members involved in the evaluation activities, including their responsibilities in planning and development, their qualifications and training programmes and managerial duties.

2.4.5 Staff members are expected to demonstrate their technical competencies, either by proof of qualification from another scheme within the CCRA, a written test or other appropriate means.

2.4.6 At any point in time, if CSA is not satisfied with or has concerns regarding the technical competencies of an evaluator, CSA reserves the right to further assess the staff, which could be in the form of a verbal interview with the staff, a written or practical test, or by any other appropriate means.

2.5 Environmental Conditions

2.5.1 The CCTL shall ensure the environment in which it operates will not affect the correctness, reliability and confidentiality of evaluation deliverables and results of the IT security testing and evaluation. For instance, access to and use of the CCTL premises must be controlled with effective separation of IT security testing and evaluation activities from other incompatible activities.

2.6 Methods

2.6.1 The CCTL shall use methodology for each evaluation task that

conforms to the CC CEM, cPP, relevant supporting documents and any other applicable international or regional standards. All methods, procedures or instructions used in the IT security testing and evaluation shall be documented.

2.6.2 The CCTL shall ensure that specialised tools used in the IT security testing and evaluation are identifiable, subject to specific configuration management, and for the testing and evaluation results to be reproducible.

2.6.3 The CCTL shall retain all records relating to the IT security evaluations, including records of original observations, derived data and other relevant information, to establish an audit trail.

2.7 Security Policy

2.7.1 The CCTL shall have and shall comply with a security policy which sets out the responsibilities of the CCTL staff members and the procedures to be undertaken by them to maintain the high degree of security required to protect commercially sensitive information. The security policy should specify procedures for human resources security, physical and environmental security, communications and operations management and access control preferably with reference to the ISO/IEC 27001/2 standard. The security policy shall be maintained by the security manager of the CCTL.

2.7.2 As the CCTL may access sensitive or proprietary information in relation to the IT product, the CCTL shall ensure that a Non-Disclosure or similar agreement is signed between the CCTL and the sponsor or developer (if applicable) and ensure that the CCTL and its staff comply with the terms of such an agreement. Such agreement shall allow any disclosure of information by the CCTL to CSA where the information is related to CSA's functions and duties as an Evaluation Authority. All relevant documents generated during the evaluation process shall be labelled with a clear protective marking and a unique identifier, e.g. as 'confidential'. This is to ensure that the sensitive documents are traceable, limited and accessible to CCTL staff members on a need-to-know basis.

3 OTHER OBLIGATIONS OF PROVISIONAL APPROVED AND APPROVED CCTL

3.1.1 The Singapore Accreditation Council (SAC), under the aegis of Enterprise Singapore, is the national accreditation body responsible for accreditation of conformity assessment activities such as certification, testing, calibration and inspection in Singapore. SAC is supported by five Council Committees and fifteen Technical Committees to manage its accreditation schemes.

3.1.2 CSA provides support to the SAC accreditation (i.e. ISO/IEC 17025) by being represented at the SAC technical committee for assessment of testing laboratories, and by providing technical assessors to its CCTL assessment team. This gives confidence that the IT security evaluations carried out by the CCTL under the SCCS are done within an accredited quality management system by independent and experience evaluators. Where necessary, CSA also issues additional guidance to the CCTL.

3.1.3 The CCTL shall maintain the ISO/IEC 17025 accreditation status at all times, and continue to comply with the stipulated requirements for the CCTL approval in this document.

3.1.4 The CCTL shall have a legally binding contractual basis (Letter of CCTL Approval and CCTL's Letter of Acceptance) with CSA.

3.1.5 For each individual certification procedure, the CCTL shall be able to present a legally enforceable agreement with the applicant that allows the CCTL to perform all examinations necessary in the context of the requested certification procedure at least to the degree of assessment envisaged in the Certification Application Form. Among other things, this agreement must cover drawing up a plan for the evaluation activities (evaluation work plan - EWP) by the CCTL, so that the necessary rules of the relevant certification program can be applied.

3.1.6 The CCTL must document the results of all evaluation activities. This documentation is drawn up in the form of evaluation, audit, inspection or observation reports. These reports must address every single aspect of evaluation that is required in the certification program and is applicable to the specific certification procedure, and clearly document the evaluation results for each aspect of evaluation.

3.1.7 The CCTL shall ensure that its IT security evaluations are performed in accordance with the procedures, rules and policies of CSA set out in the SCCS Publications #1 to #3.

3.1.8 The CCTL shall not sub-contract, outsource or assign its rights or obligations without the prior written consent of CSA. Where CSA consents to any subcontracting of work to other SCCS approved laboratories by the CCTL, the CCTL shall:

a) remain fully responsible for the performance of all evaluation tasks and be fully liable for all acts and omissions of the subcontractor;

b) be solely responsible for supervising and paying the subcontractor and ensuring the proper performance of any works by the subcontractor; and

c) ensure that the subcontractor is itself a CCTL with Provisional Approval or Approval status granted by CSA, or that the

subcontractor is otherwise qualified to perform the assigned tasks and provide CSA with such evidence of the subcontractor's qualifications and such other information as CSA deems necessary; and

d) not subcontract a major (or the full) extent of the evaluation tasks for each certification procedure.

3.1.9 The CCTL shall have a record system which provides for a retention period of 5 years for documents related to the evaluation activities. The record system shall be managed with procedures for the access to protected information, and for the creation, marking, storage, transmission, copying and disposal of protected information.

3.1.10 In addition to the audits referred to in 5.2.5, the CCTL shall be subjected to annual audits by CSA after it has been provisionally approved or approved as a CCTL under the SCCS. CSA further reserves the right to audit the CCTL's records from time to time as necessary, to verify the CCTL's compliance with the terms and conditions of the SCCS Publications #1 to #3. The CCTL shall keep complete, accurate and up to date records with respect to the evaluation activities and when requested by CSA, allow CSA to inspect, audit and/or make copies of such records. The CCTL shall allow CSA and its authorised representatives access to its premises and the right to interview its staff, sub-contractors and representatives, for the purpose of conducting such audits.

3.1.11 If any non-compliance with the terms and conditions of the SCCS Publications #1 to #3 is discovered in an audit, the CCTL shall, if so required by CSA, take corrective action as directed and pay CSA's reasonable costs in connection with the audit.

3.1.12 CSA may organise periodic feedback sessions with all CCTLs for suggestions on how the SCCS can be improved and for information sharing in evaluation techniques. The CCTLs are expected to attend such sessions. Remote approved CCTLs may opt to dial in instead of being physically present.

3.1.13 The CCTL shall <u>immediately</u> notify CSA of any of the following:

a) Changes in its legal, commercial, organisation or its ISO/IEC 17025 accreditation status;

b) Change in address of the premises where evaluations are carried out;

c) Changes which may affect the continuing compliance with any of the criteria or requirements specified under the SCCS, including movement of and changes to CCTL personnel who are directly involved in the evaluation activities or the ISO/IEC 17025 approved

signatory; and

d) Any actual or potential conflict of interest that has arisen or may arise and the details thereof.

3.1.14 CCTL shall provide an annual report to CSA by 31 December of each year. The annual report shall contain the information set out in Annex B of this document.

3.1.15 The CCTL shall fulfil its obligations to the sponsor in a timely and professional manner according to industry best standards (if any) and the terms and conditions of SCCS Publications #1 to #3. CSA may from time to time establish time limits for evaluation activities carried out under the SCCS, and the CCTL shall ensure that it complies with the timeframes specified by CSA.

3.1.16 The CCTL shall implement a clear procedure for resolving customer complaints and disputes. Upon CSA's written request, the CCTL shall make available to CSA, details of the nature of any complaints made against it and, where applicable, the resolution thereof. The CCTL shall take such corrective action as directed by CSA in respect of or as a result of any complaint.

3.1.17 The CCTL shall comply with all applicable laws and obtain and maintain all licences, consents, permits, approvals, waivers and authorisations necessary for the evaluation activities and the performance of its obligations to CSA or a sponsor under the SCCS.

3.1.18 The CCTL shall ensure that all information it provides about itself or its services and fees are true, accurate and complete, and promptly provide updates to such information.

3.1.19 The CCTL shall not purchase materials, perform services or incur costs chargeable to CSA or in any way pledge to CSA's credit.

3.1.20 The CCTL shall not make any statements or engage in conduct which brings or is likely to bring into disrepute the name and/or reputation of CSA, the SCCS, CC or the CCRA or permit anyone to do so.

3.1.21 Provisional Approval or Approval of the CCTL by CSA shall not be construed as the acceptance by CSA of any responsibility for the services provided by the CCTL. The CCTL shall not make any representation that its services are in any way guaranteed by CSA or that it is empowered to give guarantees on behalf of CSA.

3.1.22 As part of CSA's role to have oversight on the evaluation work and ensure comparability among the evaluation work performed by the CCTLs, CSA may need to attend on-site evaluation activities conducted by CCTL, whether in Singapore or overseas. Examples of circumstances where CSA may need to attend on-site evaluation

activities include but is not limited to the following:

a) Review of the Implementation Representation as part the assurance family ADV_IMP (at the developer's site(s)) and any manufacturer site(s));

b) Site-visit as part of assurance class ALC (at the developer's site(s) and any manufacturer site(s));

c) TOE testing as part of assurance class ATE; and

d) penetration testing as part of assurance class AVA.

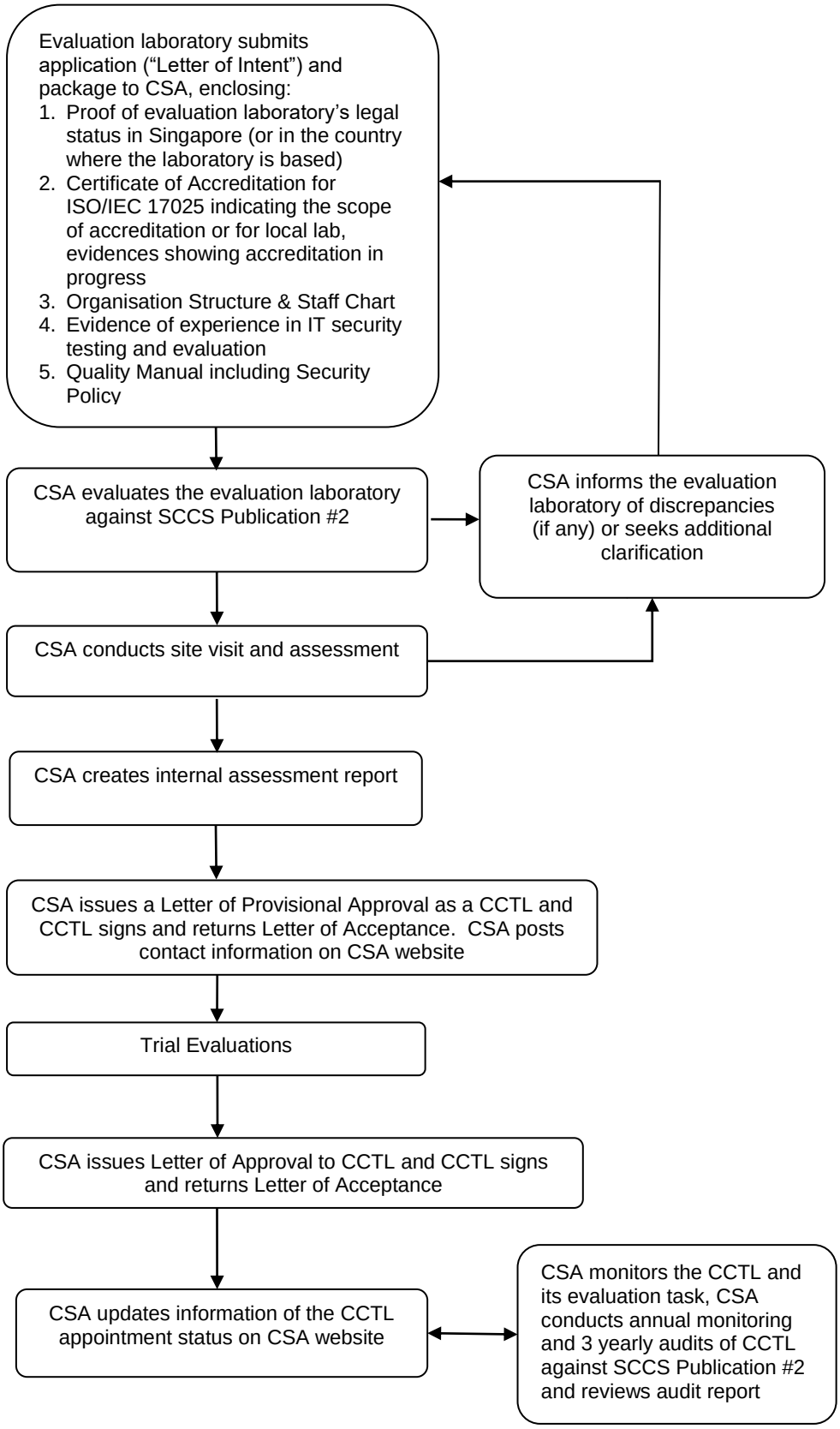
3.1.23 Where the CCTL is provisionally approved and the CCTL is performing activities (a) to (d) in section 3.1.22 for the first time under SCCS, it is likely that CSA will attend on-site.

3.1.24 The CCTL shall allow and facilitate such on-site visits by CSA (including making all necessary arrangements such as assisting with travel visa applications).

3.1.25 CSA reserves the right to determine at its absolute discretion the number and purpose of the on-site visits to be conducted in relation to any project, including the activities to be performed by the CCTL in connection with such on-site visits.

3.1.26 The CCTL shall perform a minimum of one (1) IT security evaluation activity within twelve (12) months from the date of its Approval as CCTL, and every 12 months thereafter.

4 FLOWCHART OF PROCEDURE FOR CCTL APPROVAL



5 PROCEDURE FOR APPROVAL OF CCTL

5.1 Application to be Appointed as an Approved CCTL

5.1.1 An application to be appointed as an approved CCTL should be sent by post or by e-mail and addressed to CSA at the following address:

The Technical Manager,
Singapore Common Criteria Scheme (SCCS)
5 Maxwell Road,
MND Complex, #03-00, Tower Block
Singapore 069110

or

sccs@csa.gov.sg

5.1.2 The applicant should submit the Application to be an Approved CCTL (Annex A), and the following documents:

a) Documents proving the applicant as a legal entity located and registered to do business in Singapore (or in the country where the facility is based);

b) Certificate of Accreditation by a recognised Accreditation Body as stated in 2.1.1 of this Publication, indicating in the scope of accreditation that the applicant has been accredited to ISO/IEC 17025 for testing and evaluation to the CC standards, or documents showing that the applicant has applied for such accreditation but the application is pending assessment by the Accreditation Body ;

c) Organisation structure and staffing chart;

d) Documents showing recent national and/or international experience in IT security testing and evaluation to the CC standard or equivalent; and

e) Quality Manual (including a Security Policy).

5.1.3 At the time of submission of the application to be appointed CCTL, the applicant may have applied for but yet to obtain the ISO/IEC 17025 accreditation from an Accreditation Body as stated in 2.1.1. For any avoidance of doubt, the applicant must obtain the said accreditation before the applicant can qualify for provisional approval as a CCTL.

5.1.4 The applicant may need to make arrangement for CSA's representatives to visit the applicant's premises to carry out assessments deemed necessary.

5.1.5 In order to gain confidence in the technical competencies of the staff members who will be involved in operating the CCTL, CSA may require the staff members of the applicant to be assessed as stated in 2.4.

5.1.6 If CSA is satisfied that the applicant meets the relevant qualifying criteria under the SCCS, CSA will issue to the applicant a letter of Provisional Approval as CCTL together with a Letter of Acceptance. The applicant must sign and return the Letter of Acceptance to CSA within 30 days from the date of the letter of Provisional Approval.

5.2 Provisional Approval as CCTL

5.2.1 The applicant's Provisional Approval as CCTL is valid for a period of two (2) years from the effective date stated in the Letter of Provisional Approval, or for the period commencing on the effective date stated in the Letter of Provisional Approval until Approval has been granted by CSA in accordance with 5.3, whichever is the shorter period. CSA has the sole discretion to grant the extension of the period of the applicant's Provisional Approval to up to one (1) year.

5.2.2 The CCTL must inform sponsors of IT products of its provisional status and also that such provisional approval may carry a potential risk that evaluations by the CCTL may take a longer time to be completed or require more supervision from CSA.

5.2.3 During the period of the Provisional Approval, the CCTL shall complete two (2) trial evaluations, one of which must achieve the assurance level of 4[2]. A trial evaluation is an evaluation to be performed by the CCTL under the close monitoring of CSA, which will assess whether the CCTL has demonstrated the competencies to perform evaluations according to the SCCS and the CC standards.

5.2.4 For projects which require international recognition under the CCRA, the CCTL must become ISO/IEC 17025 accredited as stated in 2.1.1 before it can issue the final and official version of its ETR to CSA.

5.2.5 Once the CCTL is able to meet the trial evaluations requirement, CSA will carry out an audit of the CCTL (which will generally follow the procedures as set out in section 8 of this Publication).

5.3 Approval as CCTL

5.3.1 A "Letter of Approval" will be issued to the CCTL when the CCTL has achieved the following:

a) Valid ISO/IEC 17025 accreditation by an Accreditation Body as

[2] This is considered fulfilled if the assurance activities are conducted for TOE conforming to a cPP which has assurance activities selected from Evaluation Assurance Levels 4, or completed the assurance activities in accordance with the National IT Evaluation Scheme (NITES) for the same TOE.

stated in 2.1.1 as at the date of the Letter;

b) Two trial evaluations for IT products completed according to requirements stipulated in 5.2.3 above, with CSA's supervision; and

c) Satisfactory outcome of the audit by CSA stated in 5.2.5.

5.3.2 The Letter of Approval will be issued together with a Letter of Acceptance. The CCTL must sign and return the Letter of Acceptance to CSA within 30 days from the date of the Letter of Approval.

5.4 Suspension or Termination of Approval as CCTL

5.4.1 CSA is entitled to suspend or terminate the approval (whether a provisional approval or approval) of a CCTL forthwith if:

a) The CCTL is in breach of any terms of SCCS Publication #1 to #3;

b) The CCTL fails to submit an application for approval as a CCTL within the stipulated time period when required by CSA under 5 of this Publication;

c) The CCTL fails to comply with the instructions of CSA during the conduct of the audit described in section 8 of this Publications;

d) The CCTL fails to prepare the action plan pursuant to the audit in section 8 or fails to comply with the said action plan to the satisfaction of CSA during the grace period granted by CSA;

e) The CCTL has not performed any IT security evaluation activity for a period of twelve (12) months without reasonable excuse;

f) The CCTL misuses the approval status or any proprietary names and marks associated with CSA, SCCS, CC or CCRA;

g) The CCTL makes any statement that misrepresents the conclusion of any evaluation or effect of its approval status;

h) CSA finds that the CCTL was in a position of conflict that impaired or would tend to impair its ability to conduct a fair and impartial evaluation under the SCCS;

i) The CCTL fails to notify CSA of the matters described in 3.1.13;

j) The CCTL fails to demonstrate the level of technical proficiency required (as described in 2.1.4, 2.1.5 and 2.1.6) to conduct security evaluation;

k) The positions of the CCTL's key technical personnel (as described in 2.3.2 and 2.4.1) are left vacant with [no suitable replacements/no

attempts to employ suitable replacements] for a period of more than 12 months;

l) The CCTL fails to repair or replace critical equipment used in the evaluation of products within the scope of its approval such that it is unable to conduct such evaluation, for a period of more than 12 months;

m) The CCTL fails to address and resolve complaints from Sponsors, Developers, customers, SAC, or other relevant parties;

n) The CCTL suspends or ceases or threatens to suspend or cease its business or becomes or threatens to become or is in jeopardy of becoming subject to any form of bankruptcy or insolvency administration or goes into liquidation (except for staff members' voluntary liquidation pursuant to reconstruction, amalgamation or reorganisation) or makes any arrangement or composition with its creditor(s) or has a receiver appointed of all or any part of its assets or takes or suffers any similar action in consequence of a debt; or

o) CSA determines there is just cause for withdrawing the CCTL's approval under the SCCS.

5.4.2 Without prejudice to section 5.4.1, CSA may suspend or terminate the CCTL's approval by giving the CCTL one (1) month's prior written notice of the suspension or termination.

5.4.3 In the event of a serious breach, the CCTL's approval may be terminated immediately by Evaluation Authority in writing. A serious breach shall be deemed to have been committed if, false representations are made by the CCTL in relation to recognition criteria under the process instructions, in evaluation reports or technical documents, or where information is not disclosed by the CCTL to CSA.

5.4.4 Upon the suspension or termination of its approval as a CCTL, the evaluation laboratory shall immediately cease all use of any proprietary names and marks associated with CSA, SCCS or CC and desist from holding itself out as a CCTL under the SCCS.

5.4.5 The evaluation laboratory shall not undertake any security evaluation or issue any evaluation reports in accordance with the SCCS during the period of suspension or after its approval has been terminated.

5.4.6 A CCTL whose approval has been terminated will be removed from the list of approved CCTLs (published on the CSA website) and any projects conducted on or after the date of termination will not result in certification under the SCCS.

5.4.7 A CCTL whose approval has been suspended will be listed as 'suspended' in the list of approved CCTLs (published on the CSA

website) and, unless otherwise specified in writing by CSA, projects conducted or continued during the suspension period will not result in certification under the SCCS.

5.4.8 A CCTL whose approval has been suspended must take required corrective measures within the time frame given by CSA. The period of suspension of a CCTL shall not be longer than twelve (12) months, and if the required corrective measures has still not been taken, CSA may terminate the approval as CCTL.

5.4.9 Any approved CCTL may voluntarily withdraw from the SCCS by giving one (1) month's written notice to CSA.

5.4.10 A CCTL whose approval has been withdrawn shall return all documents requested by CSA within seven (7) days of receiving such request.

5.5 Changes to Scope of CCTL Approval

5.5.1 Any approved CCTL may apply to CSA to increase or reduce its approved scope as a CCTL as defined in the Letter of Approval as a CCTL.

5.5.2 Such application shall be done in accordance with the procedure for Approval of CCTL as described in section 5.1, 5.2 and 5.3 of this Publication.

6 CHANGES TO PUBLICATIONS AND CONDITIONS FOR CCTL APPROVAL

6.1.1 CSA reserves the right to make changes to the SCCS Publications #1 to #3 and to impose any new conditions for the approval of CCTLs under the SCCS.

CSA may in such a case, require the CCTL to submit a fresh application (within 30 days from the date of request by CSA) to be appointed as an Approved CCTL and CSA may then assess the CCTL in accordance with the procedure set out in section 5.

7 FEES

7.1 General Policy

7.1.1 The fees for CSA's work in connection with the CCTL approving process shall be prescribed by CSA and published on the CSA website. CSA reserves the right to review the fees as and when necessary.

7.1.2 All fees are in Singapore dollars and are subjected to Goods and

Services Tax (GST).

7.1.3 The fees are payable to CSA upon the submission of the Application to be Appointed as an Approved CCTL to CSA pursuant to 5.1.

7.1.4 The application fees shall lapse after one year and the application fees are non-refundable.

8 PROCEDURE FOR AUDITING CCTL

8.1 Purpose

8.1.1 The purpose of the audit is to ensure that the CCTL is in compliance with the requirements of the SCCS Publications.

8.2 Scope of Audit

8.2.1 An audit will be conducted by CSA to ascertain the proficiency of the CCTL's personnel, CCTL personnel's compliance to CCTL procedures , equipment including but not limited to software and hardware used by the CCTL for the purposes of evaluation of products within the scope of its approval (see 5.4.1(l)) and on the following documents maintained by the CCTL :

a. The Quality Manual and other processes under the ISO/IEC 17025 and the security policy of the CCTL together with any relevant procedures and instructions;

b. Previous audit report, if any; and

c. Any information, observation reports and feedback gathered by the CCTL during the evaluations performed by the CCTL in the previous year.

8.3 Audit Proceedings

8.3.1 An opening meeting will be held on the same day before the commencement of the audit to:

a. Brief staff members of the CCTL of the purpose for the audit as well as the scope and manner in which the audit will be conducted;

b. Confirm the agenda of the audit;

c. Ensure that all staff members of the CCTL involved in the evaluation activities will be available to attend the audit.

8.3.2 Interviews with staff members

a. The purpose for the interviews is to gather information to ensure compliance with requirements as defined in the SCCS Publications.

8.3.3 Proficiency Test

a. Any staff member of the CCTL may be required to undertake a written or practical test to ascertain that staff member's technical competency.

8.3.4 Closing Meeting

a. All staff members of the CCTL should attend the audit closing meeting, including managerial and technical personnel, and any staff members interviewed during the audit.

b. During this meeting, CSA will inform the CCTL of its observations and findings from the audit. These observations and findings will form the basis for the audit report.

8.4 Post Audit

8.4.1 Audit Report

a. CSA shall prepare an audit report which will state its findings from the audit. The audit report aims to contribute to the ongoing improvement of the CCTL, affirming its strengths, pointing out areas that need to be improved and/or corrected.

b. The audit report shall be given to the CCTL.

8.4.2 Action Plan

a. Where the audit report states findings of any non-compliance of the SCCS Publications by the CCTL, the CCTL shall prepare an action plan with its proposed corrective action to address these findings.

b. The action plan shall be submitted to CSA for approval within two (2) weeks of the CCTL receiving the audit report.

c. If CSA finds that the action plan does not sufficiently address the findings in the audit report, CSA reserves the right to reject the action plan and call for an amended action plan by the CCTL to be submitted to CSA for its approval within two (2) weeks of the CCTL being notified by CSA.

8.4.3 Monitoring of Action Plan

a. Upon the approval of the action plan, CSA shall grant the CCTL a grace period for the implementation of and compliance with the action plan. CSA shall monitor the CCTL regularly during this period.

9 REFERENCES

[1] International Organization for Standardization, International Electrotechnical Commission. ISO/IEC 17025:2017 *General requirements for the competence of testing and calibration laboratories.*

[2] Singapore Accreditation Council. *Accreditation Process, SAC-Singlas 001.* May 2021.

[3] Singapore Accreditation Council. *General Requirements for the Accreditation of Information Technology Security Testing Laboratories, IT 001.* Singapore, April 2018.

[4] Singapore Accreditation Council. *Laboratory Assessment Checklist.* Singapore, April 2018.

[5] SCCS Publication 1 – *Overview of the Scheme.* Version 8.0, June 2024

[6] SCCS Publication 3 – *Information Technology Security Evaluation and Certification.* Version 8.0, June 2024

[7] Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, July 2, 2014.

[8] Common Criteria for Information Technology Security Evaluation – Part 1: *Introduction and general model*. November 2022 CC:2022 Revision 1.

[9] Common Criteria for Information Technology Security Evaluation – Part 2: *Security functional components*. November 2022 CC:2022 Revision 1.

[10] Common Criteria for Information Technology Security Evaluation – Part 3: *Security assurance components*. November 2022 CC:2022 Revision 1.

[11] Common Criteria for Information Technology Security Evaluation – Part 4: *Framework for the specification of evaluation methods and activities*. November 2022 CC:2022 Revision 1.

[12] Common Criteria for Information Technology Security Evaluation – Part 5: *Pre-defined packages of security requirements*. November 2022 CC:2022 Revision 1.

[13] Common Methodology for Information Technology Security Evaluation – *Evaluation Methodology.* November 2022 CEM:2022 Revision 1.

[14] Assurance Continuity – *CCRA Requirements*. June 2012 Version 2.1

10 ACRONYMS

The following acronyms are used in CSA Publication 1,2 and 3:

AC	Assurance Continuity
AR	Activity Report
CC	Common Criteria for Information Technology Security Evaluation
CCTL	Common Criteria Testing Laboratory
CCRA	Common Criteria Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security
CEM	Common Evaluation Methodology
CAF	Certification Application Form
CPL	Certified Product List
CR	Certification Report
CSA	Cyber Security Agency of Singapore
EAL	Evaluation Assurance Level
EPM	Evaluation Progress Meetings
ETR	Evaluation Technical Report
EWP	Evaluation Work Plan
FIPS	Federal Information Processing Standards
IAR	Impact Analysis Report
IP	Intellectual Property
MC	Management Committee
OR	Observation Report
PP	Protection Profile
RR	Review Report

SAC	Singapore Accreditation Council
SAR	Security Assurance Requirement
SCCS	Singapore Common Criteria Scheme
SFR	Security Functional Requirement
SMT	Senior Management Team
ST	Security Target
TKM	Task Kick-off Meeting
TOE	Target of Evaluation

Annex A

Sample of Application to be Approved CCTL

Company Letter Head

<Date>

Cyber Security Agency of Singapore (CSA)
5 Maxwell Road,
MND Complex, #03-00, Tower Block
Singapore 069110

Attn: Technical Manager,
Singapore Common Criteria Scheme

Dear Sir,

APPLICATION TO BE AN APPROVED CCTL UNDER THE SCCS

Our Company ***<COMPANY NAME>*** desires to be appointed as an approved Common Criteria Test Laboratory under the Singapore Common Criteria Scheme (SCCS) managed by Cyber Security Agency of Singapore Evaluation Authority (CSA).

We agree to comply with the requirements of the SCCS and the ***<Singapore Accreditation Council (SAC) (or by the local authority where the facility is based)>***.

We also agree to comply with the requirements in the SCCS Publications available on the CSA website (www.csa.gov.sg), in particular SCCS Publication Number 2 at paragraph 5.1 on the Application to be Appointed as an Approved CCTL. We enclose all requested documentation in compliance with the said paragraph.

Should we subsequently be provisionally or fully appointed as a CCTL, we agree to comply with and bound by all requirements in the SCCS Publications.

The details of our point of contact for this application are as follows:

<CONTACT NAME>
<TITLE>
<PHONE>
<E-MAIL ADDRESS>
<COMPANY NAME>
<REGISTRATION NUMBER>
<COMPANY ADDRESS>

Sincerely,

<NAME>
<TITLE>

Annex B

Annual Report

The annual report referred to in section 3.1.14 shall contain at least the following information:

a) Report on all projects and evaluations conducted under the SCCS for the reporting calendar year
   i. Status per projects (ongoing or finished during the year)
   ii. Concerns on the project
   iii. Information about the project progress
   iv. Staff assignments, changes, or partial work on projects

b) Information about the testing laboratory
   i. Staff who have left during the year
   ii. New evaluation staff who have joined during the year
   iii. Changes in organisational structure or management
   iv. Changes in office location
   v. Special (mandatory) training attended by staff
   vi. New dedicated (special) tools or equipment (purchased or in plan to be purchased)

c) Information about accreditations
   i. Audits by external bodies and results
   ii. ISO 17025 (accreditation) status/ renewal (submission of certificate)
   iii. Changes regarding the ISO 17025 signatory

d) Feedback to CSA on any concerns or suggestions for improvement for the SCCS

e) Feedback on business opportunities and perceived market situation

f) Any other information that the CSA may require and has communicated to the CCTL in writing