Cybersecurity Labelling Scheme

FOR MEDICAL DEVICES

BY CYBER SECURITY AGENCY OF SINGAPORE

Cybersecurity Labelling Scheme for Medical Devices [CLS(MD)] Publication No. 3

Requirements for Testing Laboratory

October 2023
Version 0.3

FOREWORD

The Cybersecurity Labelling Scheme for Medical Devices [CLS(MD)] is part of efforts from the Ministry of Health (MOH), Cyber Security Agency (CSA), Health Sciences Authority (HSA), and Synapxe to better secure Singapore's cyberspace and to raise cyber hygiene levels in medical devices.

Under the CLS(MD), the cybersecurity label for medical devices would provide an indication of the level of security in medical devices. It aims to improve security awareness by making such provisions more transparent to healthcare users and empowers them to make informed purchasing decisions for medical devices with better security using the information on the cybersecurity label.

The CLS(MD) seeks to incentivise manufacturers to develop and provide medical devices with enhanced cybersecurity provisions. The labels also serve to differentiate medical devices with better cybersecurity safeguards in the market, from their competitors.

At the same time, CSA intends to engage other like-minded partners for mutual recognition of the CLS(MD) with the objective of eliminating duplicated assessments across national boundaries.

The CLS(MD) is managed by the Cybersecurity Certification Centre (CCC) under the ambit of the Cyber Security Agency of Singapore (CSA). The CLS(MD) is jointly owned by MOH and CSA.

Amendment Record

Version	Date	Author	Changes
0.3	October 2023	Cyber Security Agency of Singapore	Draft

Contents

NOTICE

The Cyber Security Agency of Singapore makes no warranty of any kind with regard to this material and shall not be liable for errors contained herein or for incidental or consequential damages in connection with the use of this material.

1 INTRODUCTION

1.0.1 The Cybersecurity Certification Centre (CCC) of the Cyber Security Agency of Singapore (CSA) is responsible for approving Testing Laboratories (TL) to perform the evaluation activities defined for level 3 and level 4 of the Cybersecurity Labelling Scheme for Medical Devices [CLS(MD)].

1.0.2 Any testing laboratory that conducts, or intends to conduct, the business of security testing and evaluation under the CLS(MD), must apply to CSA for approval to be a TL.

1.0.3 To be an approved TL for CLS(MD), the TL shall either:

- be an approved Common Criteria Testing Laboratory under the Singapore Common Criteria Scheme (https://www.csa.gov.sg/sccs), eligible to perform CLS(MD) evaluation activities up to Level 4;
- be an approved Testing Laboratory under the Cybersecurity Labelling Scheme for IoT(https://www.csa.gov.sg/cls-iot), eligible to perform CLS(MD) evaluation activities up to Level 3, or up to Level 4 via a technical assessment through the conduct of 1 trial evaluation at Level 4;
- or assessed by CSA to have fulfilled all the requirements specified in this document.

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 TL.

2 ELIGIBILITY CRITERIA

2.1 General Requirements

2.1.1 The testing 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/ICT/IoT security. 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/).

[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.

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 security requirements for handling protected information that CSA may disclose to the laboratory and those of which relating to their customers' 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 to meet the requirements of this document and to satisfy the needs of the customer.

2.1.4 The testing 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.

3 OBLIGATIONS OF THE APPROVED TEST LABORATORY

3.1 General Obligations

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

3.1.2 For each individual CLS(MD) level 3 or level 4 procedure, the TL shall be able to present, when requested by CSA, a legally enforceable agreement with its customer that allows the TL to perform all examinations necessary in the context of the requested CLS(MD) procedure.

3.1.3 The TL must document the results of all evaluation activities. This documentation is drawn up in the form of evaluation reports. These reports must address all aspects of the evaluation that is required in the CLS(MD) procedure, and clearly document the evaluation results for each aspect of evaluation.

3.1.4 The TL shall ensure that its security evaluations are performed in accordance with the procedures, rules and policies set out by CSA in the CLS(MD) Publications, which are publicly available on the CLS(MD) website (https://www.csa.gov.sg/cls-md).

3.1.5 The TL 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, the TL 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;

c) ensure that the subcontractor is 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 CLS(MD) procedure.

3.1.6 CSA reserves the right to audit the TL's records from time to time as necessary, to verify the TL's compliance with the terms and conditions set forth in the CLS(MD) Publications. The TL 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 TL 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.

3.1.7 If any non-compliance with the terms and conditions is discovered in an audit, the TL shall, if so required by CSA, take corrective action as directed and pay CSA's reasonable costs in connection with the audit.

3.1.8 The TL shall immediately 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 CLS, including movement of and changes to the key personnel who are directly involved in the evaluation activities; and

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

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

3.1.10 The TL 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 its customers under the CLS(MD).

3.1.11 The TL 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.

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

3.1.13 The TL 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 CLS(MD), or permit anyone to do so.

3.1.14 The TL 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.

3.2 ISO/IEC 17025

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

3.3 Staff Members

3.3.1 The laboratory shall be responsible for ensuring that all staff members who perform specific evaluation activities have the relevant cybersecurity qualifications, training, experience, and demonstrated skills.

3.3.2 Staff members are expected to demonstrate their technical competencies, either by proof of qualification, a written test, or other means as deemed appropriate by CSA.

3.3.3 At any point in time, if CSA is not satisfied with or has concerns regarding the technical competencies of the staff involved in the security evaluation activities for CLS(MD) Level 3 or Level 4, 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.

3.4 Impartiality

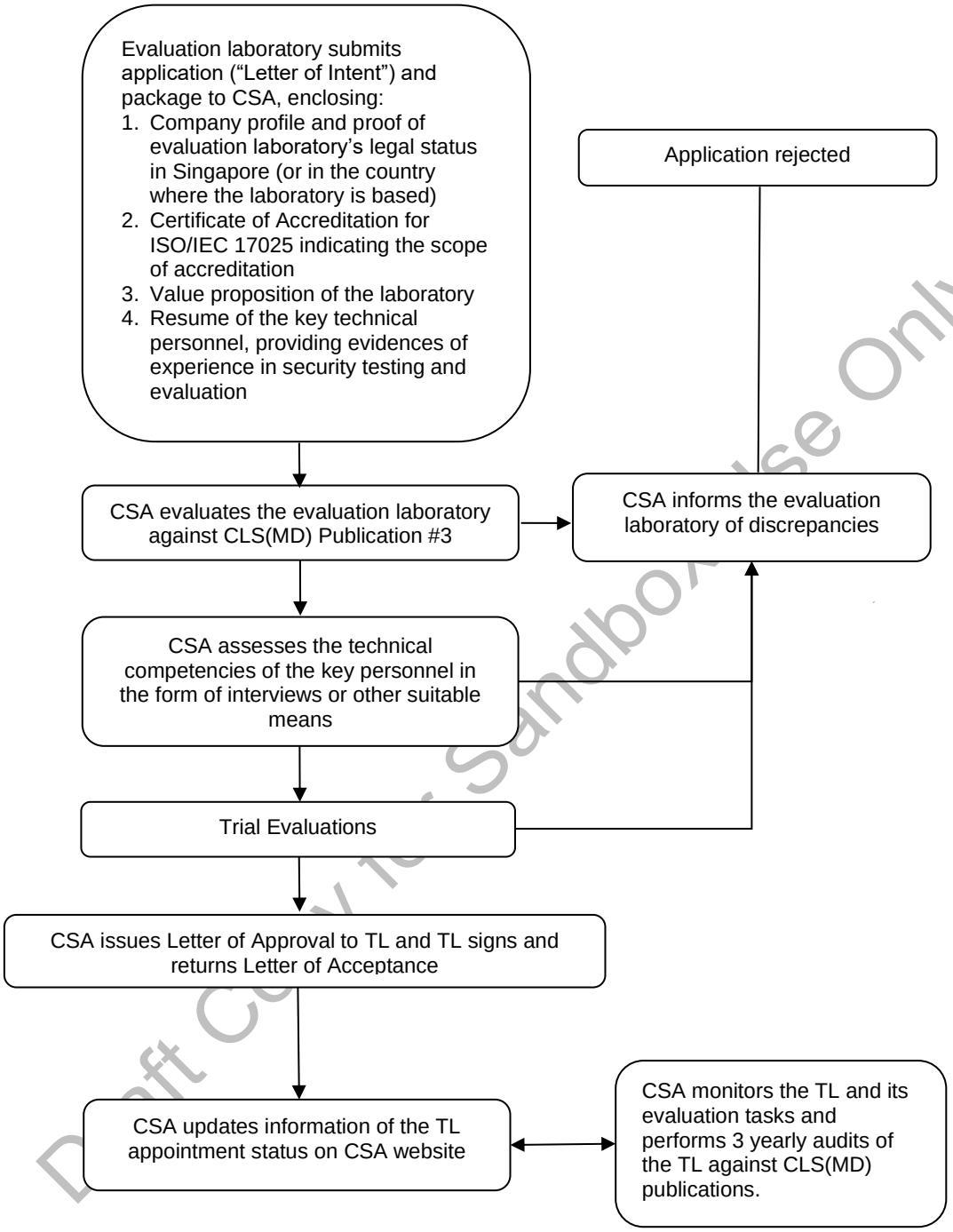
3.4.1 If the TL is part of an organisation that performs activities other than IT security evaluation (e.g. consultation to product manufacturer), the TL shall identify actual and potential conflicts of interest and ensure clear

separation of control to ensure that there is no undue influence on the evaluation activities.

3.4.2 The TL 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.

3.4.3 For every project carried out under the CLS(MD), the TL shall declare in the form of writing, 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.

4 FLOWCHART OF PROCEDURE FOR TL APPROVAL



5 PROCEDURE FOR APPROVAL OF TL FOR CLS

5.1 Application to be Appointed as an Approved TL

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

The Technical Manager,
Cybersecurity Labelling Scheme for Medical Devices [CLS(MD)]
CSA Cybersecurity Certification Centre
5 Maxwell Road,
MND Complex, #03-00, Tower Block
Singapore 069110

or

cls_md@csa.gov.sg

5.1.2 The applicant should submit the Letter of Intent (Annex A), and the following documents:

a) Company Profile and 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 relevant standard;

c) A writeup detailing:

a. the applicant's business plan with respect to CLS(MD), and synergy of CLS(MD) with its current business;
b. the value proposition the applicant could bring to the scheme, including proliferation, adoption, future development of CLS(MD) and synergy with its current business;
c. the proposed charges for CLS(MD) level 3 and level 4; and
d. build up plan in growing cybersecurity assurance expertise, such as Common Criteria, Cybersecurity Labelling Scheme for Medical Device, and other penetration testing capabilities.

d) Resume of the key personnel and relevant information demonstrating experience in security testing and evaluation to the relevant standards.

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

5.1.4 In order to gain confidence in the technical competencies of the staff members, CSA may require the staff members of the applicant to be assessed via an interview, a written test or other means as deemed appropriate.

5.1.5 The applicant shall complete trial evaluation to demonstrate technical competency. If the applicant desires to be an approved TL for CLS(MD) Level 3, the applicant shall complete a trial evaluation at Level 3. If the applicant desires to be an approved TL for CLS(MD) Levels 3 and 4, the applicant shall complete a trial evaluation at Level 4. The applicant is expected to source for the trial evaluations. The applicant shall, without ambiguity, make known to the manufacturer(s) that their product(s) is/are being submitted as trial evaluations and carries potential risk that the evaluations may take a longer time to be completed or may not achieve the label at the end of the procedure.

5.1.6 The trial evaluations will be subjected to more stringent review and close monitoring by CSA, which will assess whether the applicant has demonstrated the competencies to perform evaluations according to the CLS(MD) requirements. The applicant is expected to demonstrate the tests conducted.

5.1.7 If CSA is satisfied that the applicant meets the relevant qualifying criteria under the CLS(MD), CSA will issue to the applicant a Letter of Approval 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 Approval.

5.2 Suspension or Termination of Approval as TL

5.2.1 CSA is entitled to suspend or terminate the approval of a TL forthwith if:

a) the TL is in breach of any terms of CLS(MD) Publications;

b) the TL has not performed any CLS(MD) evaluations for a period of twelve (12) months without reasonable justifications;

c) the TL misuses the approval status or any proprietary names and marks associated with CSA, CCC or CLS(MD);

d) the TL makes any statement that misrepresents the conclusion of any evaluation or effect of its approval status;

e) CSA finds that the TL was in a position of conflict that impaired or may impair its ability to conduct a fair and impartial evaluation under the CLS(MD);

f) the TL fails to notify CSA of the matters described in 3.1.8;

g) the TL fails to demonstrate the level of technical proficiency required

as described 2.1.4 to conduct security evaluation;

h) the positions of the TL's key technical personnel are left vacant with no suitable replacements or no attempts to employ suitable replacements for a period of more than 12 months;

i) the TL fails to address and resolve complaints from customers, SAC, or other relevant parties;

j) the TL 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

k) CSA determines there is just cause for withdrawing the TL's approval under the CLS(MD).

5.2.2 Without prejudice to section 5.2.1, CSA may suspend or terminate the TL's approval by giving the TL one (1) month's prior written notice of the suspension or termination.

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

5.2.4 Upon the suspension or termination of its approval as a TL, the evaluation laboratory shall immediately cease all use of any proprietary names and marks associated with CSA, CCC, or CLS(MD), and desist from holding itself out as a TL under the CLS(MD).

5.2.5 The evaluation laboratory shall not undertake any security evaluation or issue any evaluation reports in accordance with the CLS(MD) during the period of suspension or after its approval has been terminated.

5.2.6 A TL whose approval has been terminated will be removed from the list of approved TLs (published on the CSA website) and any projects conducted on or after the date of termination will not result in the issuance of any label under the CLS(MD).

5.2.7 A TL whose approval has been suspended will be listed as 'suspended' in the list of approved TLs (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 issuance of any label under

the CLS(MD).

5.2.8 A TL whose approval has been suspended must take required corrective measures within the time frame given by CSA. The period of suspension of a TL 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 TL.

5.2.9 Any approved TL may voluntarily withdraw from the CLS(MD) by giving one (1) month's written notice to CSA.

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

6 CHANGES TO PUBLICATIONS AND CONDITIONS FOR TL APPROVAL

6.1.1 CSA reserves the right to make changes to the CLS(MD) Publications and to impose any new conditions for the approval of TLs under the CLS(MD).

6.1.2 CSA may in such a case, require the TL to submit a fresh application (within 30 days from the date of request by CSA) to be appointed as an Approved TL and CSA may then assess the TL 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 TL 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 the prevailing 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 TL 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 REFERENCES

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

[2] Singapore Accreditation Council. *Accreditation Process, SAC-Singlas 001.* Feburary 2017.

[3] Singapore Accreditation Council. *Requirements for the Application of ISO/IEC 17025, SAC-Singlas 002.* Singapore, Feburary 2017.

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

[5] Singapore Accreditation Council. *Laboratory Assessment Checklist.* Singapore, Feburary 2017.

Annex A

Sample of Letter of Intent

Company Letter Head

<Date>

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

Attn: Technical Manager,
Cybersecurity Labelling Scheme for Medical Devices

Dear Sir/Mdm,

APPLICATION TO BE AN APPROVED TL UNDER THE CLS(MD)

Our Company ***<COMPANY NAME>*** desires to be appointed as an approved Test Laboratory under the Cybersecurity Labelling Scheme for Medical Devices [CLS(MD)] managed by Cyber Security Agency of Singapore (CSA)'s Cybersecurity Certification Centre (CCC).

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

We also agree to comply with the requirements in the CLS(MD) Publications available on the CSA website (www.csa.gov.sg/cls-md), in particular CLS(MD) Publication Number 3 on the Application to be Appointed as an Approved TL. We enclose all requested documentation in compliance with the said paragraph.

Should we subsequently be appointed as a TL, we agree to comply with and bound by all requirements in the CLS(MD) 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>